National Security Agency

Cybersecurity and Infrastructure Security Agency

Joint Cybersecurity Advisory

TLP:CLEAR

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

A plea for network defenders and software manufacturers to fix common problems.

Executive summary

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

These misconfigurations illustrate (1) a trend of systemic weaknesses in many large organizations, including those with mature cyber postures, and (2) the importance of software manufacturers embracing secure-by-design principles to reduce the burden on network defenders:

- Properly trained, staffed, and funded network security teams can implement the known mitigations for these weaknesses.

- Software manufacturers must reduce the prevalence of these misconfigurations—thus strengthening the security posture for customers—by incorporating secure-by-design and -default principles and tactics into their software development practices.[1]

NSA and CISA encourage network defenders to implement the recommendations found within the Mitigations section of this advisory—including the following—to reduce the risk of malicious actors exploiting the identified misconfigurations.

- Remove default credentials and harden configurations.
- Disable unused services and implement access controls.
- Update regularly and automate patching, prioritizing patching of known exploited vulnerabilities.[2]
- Reduce, restrict, audit, and monitor administrative accounts and privileges.

NSA and CISA urge software manufacturers to take ownership of improving security outcomes of their customers by embracing secure-by-design and-default tactics, including:

- Embedding security controls into product architecture from the start of development and throughout the entire software development lifecycle (SDLC).
- Eliminating default passwords.
- Providing high-quality audit logs to customers at no extra charge.
- Mandating MFA, ideally phishing-resistant, for privileged users and making MFA a default rather than opt-in feature.[3]

Contents

Tables

Technical details

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 13, and the MITRE D3FEND™ cybersecurity countermeasures framework.[4],[5] See the Appendix: MITRE ATT&CK tactics and techniques section for tables summarizing the threat actors' activity mapped to MITRE ATT&CK tactics and techniques, and the Mitigations section for MITRE D3FEND countermeasures.

For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.[6],[7]

Overview

Over the years, the following NSA and CISA teams have assessed the security posture of many network enclaves across the Department of Defense (DoD); Federal Civilian Executive Branch (FCEB); state, local, tribal, and territorial (SLTT) governments; and the private sector:

- Depending on the needs of the assessment, NSA Defensive Network Operations (DNO) teams feature capabilities from Red Team (adversary emulation), Blue Team (strategic vulnerability assessment), Hunt (targeted hunt), and/or Tailored Mitigations (defensive countermeasure development).
- CISA Vulnerability Management (VM) teams have assessed the security posture of over 1,000 network enclaves. CISA VM teams include Risk and Vulnerability Assessment (RVA) and CISA Red Team Assessments (RTA).[8] The RVA team conducts remote and onsite assessment services, including penetration testing and configuration review. RTA emulates cyber threat actors in coordination with an organization to assess the organization's cyber detection and response capabilities.
- CISA Hunt and Incident Response teams conduct proactive and reactive engagements, respectively, on organization networks to identify and detect cyber threats to U.S. infrastructure.

During these assessments, NSA and CISA identified the 10 most common network misconfigurations, which are detailed below. These misconfigurations (non-prioritized) are systemic weaknesses across many networks.

Many of the assessments were of Microsoft® Windows® and Active Directory® environments. This advisory provides details about, and mitigations for, specific issues found during these assessments, and so mostly focuses on these products. However, it should be noted that many other environments contain similar misconfigurations. Network owners and operators should examine their networks for similar misconfigurations even when running other software not specifically mentioned below.

1. Default configurations of software and applications

Default configurations of systems, services, and applications can permit unauthorized access or other malicious activity. Common default configurations include:

- Default credentials
- Default service permissions and configurations settings

Default credentials

Many software manufacturers release commercial off-the-shelf (COTS) network devices—which provide user access via applications or web portals—containing predefined default credentials for their built-in administrative accounts.[9] Malicious actors and assessment teams regularly abuse default credentials by:

- Finding credentials with a simple web search [T1589.001] and using them [T1078.001] to gain authenticated access to a device.
- Resetting built-in administrative accounts [T1098] via predictable forgotten passwords questions.
- Leveraging default virtual private network (VPN) credentials for internal network access [T1133].
- Leveraging publicly available setup information to identify built-in administrative credentials for web applications and gaining access to the application and its underlying database.
- Leveraging default credentials on software deployment tools [T1072] for code execution and lateral movement.

In addition to devices that provide network access, printers, scanners, security cameras, conference room audiovisual (AV) equipment, voice over internet protocol (VoIP) phones, and internet of things (IoT) devices commonly contain default credentials that can be used for easy unauthorized access to these devices as well. Further compounding this problem, printers and scanners may have privileged domain accounts loaded so that users can easily scan documents and upload them to a shared drive or email them. Malicious actors who gain access to a printer or scanner using default credentials can use the loaded privileged domain accounts to move laterally from the device and compromise the domain [T1078.002].

Default service permissions and configuration settings

Certain services may have overly permissive access controls or vulnerable configurations by default. Additionally, even if the providers do not enable these services by default, malicious actors can easily abuse these services if users or administrators enable them.

Assessment teams regularly find the following:

- Insecure Active Directory Certificate Services
- Insecure legacy protocols/services
- Insecure Server Message Block (SMB) service

Insecure Active Directory Certificate Services

Active Directory Certificate Services (ADCS) is a feature used to manage Public Key Infrastructure (PKI) certificates, keys, and encryption inside of Active Directory (AD) environments. ADCS templates are used to build certificates for different types of servers and other entities on an organization's network.

Malicious actors can exploit ADCS and/or ADCS template misconfigurations to manipulate the certificate infrastructure into issuing fraudulent certificates and/or escalate user privileges to domain administrator privileges. These certificates and domain escalation paths may grant actors unauthorized, persistent access to systems and critical data, the ability to impersonate legitimate entities, and the ability to bypass security measures.

Assessment teams have observed organizations with the following misconfigurations:

- **ADCS servers running with web-enrollment enabled**. If web-enrollment is enabled, unauthenticated actors can coerce a server to authenticate to an actor-controlled computer, which can relay the authentication to the ADCS web-enrollment service and obtain a certificate [T1649] for the server's account. These fraudulent, trusted certificates enable actors to use adversary-in-the-middle techniques [T1557] to masquerade as trusted entities on the network. The actors can also use the certificate for AD authentication to obtain a Kerberos Ticket Granting Ticket (TGT) [T1558.001], which they can use to compromise the server and usually the entire domain.
- **ADCS templates where low-privileged users have enrollment rights, and the enrollee supplies a subject alternative name.** Misconfiguring various elements of ADCS templates can result in domain escalation by unauthorized users (e.g., granting low-privileged users certificate enrollment rights, allowing requesters to specify a `subjectAltName` in the certificate signing request [CSR],

not requiring authorized signatures for CSRs, granting `FullControl` or `WriteDacl` permissions to users). Malicious actors can use a low-privileged user account to request a certificate with a particular Subject Alternative Name (SAN) and gain a certificate where the SAN matches the User Principal Name (UPN) of a privileged account.

Note: For more information on known escalation paths, including PetitPotam NTLM relay techniques, see: Domain Escalation: PetitPotam NTLM Relay to ADCS Endpoints and Certified Pre-Owned. Active Directory Certificate Services.[10],[11],[12]

Insecure legacy protocols/services

Many vulnerable network services are enabled by default, and assessment teams have observed them enabled in production environments. Specifically, assessment teams have observed Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS), which are Microsoft Windows components that serve as alternate methods of host identification. If these services are enabled in a network, actors can use spoofing, poisoning, and relay techniques [T1557.001] to obtain domain hashes, system access, and potential administrative system sessions. Malicious actors frequently exploit these protocols to compromise entire Windows' environments.

Malicious actors can spoof an authoritative source for name resolution on a target network by responding to passing traffic, effectively poisoning the service so that target computers will communicate with an actor-controlled system instead of the intended one. If the requested system requires identification/authentication, the target computer will send the user's username and hash to the actor-controlled system. The actors then collect the hash and crack it offline to obtain the plain text password [T1110.002].

Insecure Server Message Block (SMB) service

The Server Message Block service is a Windows component primarily for file sharing. Its default configuration, including in the latest version of Windows, does not require signing network messages to ensure authenticity and integrity. If SMB servers do not enforce SMB signing, malicious actors can use machine-in-the-middle techniques, such as NTLM relay. Further, malicious actors can combine a lack of SMB signing with the name resolution poisoning issue (see above) to gain access to remote systems [T1021.002] without needing to capture and crack any hashes.

2. Improper separation of user/administrator privilege

Administrators often assign multiple roles to one account. These accounts have access to a wide range of devices and services, allowing malicious actors to move through a network quickly with one compromised account without triggering lateral movement and/or privilege escalation detection measures.

Assessment teams have observed the following common account separation misconfigurations:

- Excessive account privileges
- Elevated service account permissions
- Non-essential use of elevated accounts

Excessive account privileges

Account privileges are intended to control user access to host or application resources to limit access to sensitive information or enforce a least-privilege security model. When account privileges are overly permissive, users can see and/or do things they should not be able to, which becomes a security issue as it increases risk exposure and attack surface.

Expanding organizations can undergo numerous changes in account management, personnel, and access requirements. These changes commonly lead to privilege creep—the granting of excessive access and unnecessary account privileges. Through the analysis of topical and nested AD groups, a malicious actor can find a user account [T1078] that has been granted account privileges that exceed their need-to-know or least-privilege function. Extraneous access can lead to easy avenues for unauthorized access to data and resources and escalation of privileges in the targeted domain.

Elevated service account permissions

Applications often operate using user accounts to access resources. These user accounts, which are known as service accounts, often require elevated privileges. When a malicious actor compromises an application or service using a service account, they will have the same privileges and access as the service account.

Malicious actors can exploit elevated service permissions within a domain to gain unauthorized access and control over critical systems. Service accounts are enticing targets for malicious actors because such accounts are often granted elevated permissions within the domain due to the nature of the service, and because access to use the service can be requested by any valid domain user. Due to these factors, kerberoasting—a form of credential access achieved by cracking service account credentials—is a common technique used to gain control over service account targets [T1558.003].

Non-essential use of elevated accounts

IT personnel use domain administrator and other administrator accounts for system and network management due to their inherent elevated privileges. When an administrator account is logged into a compromised host, a malicious actor can steal and use the account's credentials and an AD-generated authentication token [T1528] to move, using the elevated permissions, throughout the domain [T1550.001]. Using an elevated account for normal day-to-day, non-administrative tasks increases the account's exposure and, therefore, its risk of compromise and its risk to the network.

Malicious actors prioritize obtaining valid domain credentials upon gaining access to a network. Authentication using valid domain credentials allows the execution of secondary enumeration techniques to gain visibility into the target domain and AD structure, including discovery of elevated accounts and where the elevated accounts are used [T1087].

Targeting elevated accounts (such as domain administrator or system administrators) performing day-to-day activities provides the most direct path to achieve domain escalation. Systems or applications accessed by the targeted elevated accounts significantly increase the attack surface available to adversaries, providing additional paths and escalation options.

After obtaining initial access via an account with administrative permissions, an assessment team compromised a domain in under a business day. The team first gained initial access to the system through phishing [T1566], by which they enticed the end user to download [T1204] and execute malicious payloads. The targeted end-user account had administrative permissions, enabling the team to quickly compromise the entire domain.

3. Insufficient internal network monitoring

Some organizations do not optimally configure host and network sensors for traffic collection and end-host logging. These insufficient configurations could lead to undetected adversarial compromise. Additionally, improper sensor configurations limit the traffic collection capability needed for enhanced baseline development and detract from timely detection of anomalous activity.

Assessment teams have exploited insufficient monitoring to gain access to assessed networks. For example:

- An assessment team observed an organization with host-based monitoring, but no network monitoring. Host-based monitoring informs defensive teams about adverse activities on singular hosts and network monitoring informs about adverse activities traversing hosts [TA0008]. In this example, the organization could identify infected hosts but could not identify where the infection was coming from, and thus could not stop future lateral movement and infections.

- An assessment team gained persistent deep access to a large organization with a mature cyber posture. The organization did not detect the assessment team's lateral movement, persistence, and command and control (C2) activity, including when the team attempted noisy activities to trigger a security response. For more information on this activity, see CSA CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks.[13]

4. Lack of network segmentation

Network segmentation separates portions of the network with security boundaries. Lack of network segmentation leaves no security boundaries between the user, production, and critical system networks. Insufficient network segmentation allows an actor who has compromised a resource on the network to move laterally across a variety of systems uncontested. Lack of network segregation additionally leaves organizations significantly more vulnerable to potential ransomware attacks and post-exploitation techniques.

Lack of segmentation between IT and operational technology (OT) environments places OT environments at risk. For example, assessment teams have often gained access to OT networks—despite prior assurance that the networks were fully air gapped, with no possible connection to the IT network—by finding special purpose, forgotten, or even accidental network connections [T1199].

5. Poor patch management

Vendors release patches and updates to address security vulnerabilities. Poor patch management and network hygiene practices often enable adversaries to discover open attack vectors and exploit critical vulnerabilities. Poor patch management includes:

- Lack of regular patching
- Use of unsupported operating systems (OSs) and outdated firmware

Lack of regular patching

Failure to apply the latest patches can leave a system open to compromise from publicly available exploits. Due to their ease of discovery—via vulnerability scanning [T1595.002] and open source research [T1592]—and exploitation, these systems are immediate targets for adversaries. Allowing critical vulnerabilities to remain on production systems without applying their corresponding patches significantly increases the attack surface. Organizations should prioritize patching known exploited vulnerabilities in their environments.[2]

Assessment teams have observed threat actors exploiting many CVEs in public-facing applications [T1190], including:

- CVE-2019-18935 in an unpatched instance of Telerik® UI for ASP.NET running on a Microsoft IIS server.[14]
- CVE-2021-44228 (Log4Shell) in an unpatched VMware® Horizon server.[15]
- CVE-2022-24682, CVE-2022-27924, and CVE-2022-27925 chained with CVE-2022-37042, or CVE-2022-30333 in an unpatched Zimbra® Collaboration Suite.[16]

Use of unsupported OSs and outdated firmware

Using software or hardware that is no longer supported by the vendor poses a significant security risk because new and existing vulnerabilities are no longer patched. Malicious actors can exploit vulnerabilities in these systems to gain unauthorized access, compromise sensitive data, and disrupt operations [T1210].

Assessment teams frequently observe organizations using unsupported Windows operating systems without updates MS17-010 and MS08-67. These updates, released years ago, address critical remote code execution vulnerabilities.[17],[18]

6. Bypass of system access controls

A malicious actor can bypass system access controls by compromising alternate authentication methods in an environment. If a malicious actor can collect hashes in a network, they can use the hashes to authenticate using non-standard means, such as pass-the-hash (PtH) [T1550.002]. By mimicking accounts without the clear-text password, an actor can expand and fortify their access without detection. Kerberoasting is also one of the most time-efficient ways to elevate privileges and move laterally throughout an organization’s network.

7. Weak or misconfigured MFA methods

Misconfigured smart cards or tokens

Some networks (generally government or DoD networks) require accounts to use smart cards or tokens. Multifactor requirements can be misconfigured so the password hashes for accounts never change. Even though the password itself is no longer used—because the smart card or token is required instead—there is still a password hash for the account that can be used as an alternative credential for authentication. If the password hash never changes, once a malicious actor has an account’s password hash [T1111], the actor can use it indefinitely, via the PtH technique for as long as that account exists.

Lack of phishing-resistant MFA

Some forms of MFA are vulnerable to phishing, “push bombing” [T1621], exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or “SIM swap” techniques. These attempts, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems. (See CISA’s Fact Sheet Implementing Phishing-Resistant MFA for more information.)[3]

For example, assessment teams have used voice phishing to convince users to provide missing MFA information [T1598]. In one instance, an assessment team knew a user’s main credentials, but their login attempts were blocked by MFA requirements. The team then masqueraded as IT staff and convinced the user to provide the MFA code over the phone, allowing the team to complete their login attempt and gain access to the user’s email and other organizational resources.

8. Insufficient ACLs on network shares and services

Data shares and repositories are primary targets for malicious actors. Network administrators may improperly configure ACLs to allow for unauthorized users to access sensitive or administrative data on shared drives.

Actors can use commands, open source tools, or custom malware to look for shared folders and drives [T1135].

- In one compromise, a team observed actors use the `net share` command—which displays information about shared resources on the local computer—and the `ntfsinfo` command to search network shares on compromised computers. In the same compromise, the actors used a custom tool, CovalentStealer, which is designed to identify file shares on a system, categorize the files [T1083], and upload the files to a remote server [TA0010].[19],[20]
- Ransomware actors have used the SoftPerfect® Network Scanner, `netscan.exe`—which can ping computers [T1018], scan ports [T1046], and discover shared folders—and SharpShares to enumerate accessible network shares in a domain.[21],[22]

Malicious actors can then collect and exfiltrate the data from the shared drives and folders. They can then use the data for a variety of purposes, such as extortion of the organization or as intelligence when formulating intrusion plans for further network compromise. Assessment teams routinely find sensitive information on network shares [T1039] that could facilitate follow-on activity or provide opportunities for extortion. Teams regularly find drives containing cleartext credentials [T1552] for service accounts, web applications, and even domain administrators.

Even when further access is not directly obtained from credentials in file shares, there can be a treasure trove of information for improving situational awareness of the target network, including the network's topology, service tickets, or vulnerability scan data. In addition, teams regularly identify sensitive data and PII on shared drives (e.g., scanned documents, social security numbers, and tax returns) that could be used for extortion or social engineering of the organization or individuals.

9. Poor credential hygiene

Poor credential hygiene facilitates threat actors in obtaining credentials for initial access, persistence, lateral movement, and other follow-on activity, especially if phishing-resistant MFA is not enabled. Poor credential hygiene includes:

- Easily crackable passwords
- Cleartext password disclosure

Easily crackable passwords

Easily crackable passwords are passwords that a malicious actor can guess within a short time using relatively inexpensive computing resources. The presence of easily crackable passwords on a network generally stems from a lack of password length (i.e., shorter than 15 characters) and randomness (i.e., is not unique or can be guessed). This is often due to lax requirements for passwords in organizational policies and user training. A policy that only requires short and simple passwords leaves user passwords susceptible to password cracking. Organizations should provide or allow employee use of password managers to enable the generation and easy use of secure, random passwords for each account.

Often, when a credential is obtained, it is a hash (one-way encryption) of the password and not the password itself. Although some hashes can be used directly with PtH techniques, many hashes need to be cracked to obtain usable credentials. The cracking process takes the captured hash of the user's plaintext password and leverages dictionary wordlists and rulesets, often using a database of billions of previously compromised passwords, in an attempt to find the matching plaintext password [T1110.002].

One of the primary ways to crack passwords is with the open source tool, Hashcat, combined with password lists obtained from publicly released password breaches. Once a malicious actor has access to a plaintext password, they are usually limited only by the account's permissions. In some cases, the actor may be restricted or detected by advanced defense-in-depth and zero trust implementations as well, but this has been a rare finding in assessments thus far.

Assessment teams have cracked password hashes for NTLM users, Kerberos service account tickets, NetNTLMv2, and PFX stores [T1555], enabling the team to elevate privileges and move laterally within networks. In 12 hours, one team cracked over 80% of all users' passwords in an Active Directory, resulting in hundreds of valid credentials.

Cleartext password disclosure

Storing passwords in cleartext is a serious security risk. A malicious actor with access to files containing cleartext passwords [T1552.001] could use these credentials to log into the affected applications or systems under the guise of a legitimate user. Accountability is lost in this situation as any system logs would record valid user accounts accessing applications or systems.

Malicious actors search for text files, spreadsheets, documents, and configuration files in hopes of obtaining cleartext passwords. Assessment teams frequently discover cleartext passwords, allowing them to quickly escalate the emulated intrusion from the compromise of a regular domain user account to that of a privileged account, such as a Domain or Enterprise Administrator. A common tool used for locating cleartext passwords is the open source tool, Snaffler.[23]

10. Unrestricted code execution

If unverified programs are allowed to execute on hosts, a threat actor can run arbitrary, malicious payloads within a network.

Malicious actors often execute code after gaining initial access to a system. For example, after a user falls for a phishing scam, the actor usually convinces the victim to run code on their workstation to gain remote access to the internal network. This code is usually an unverified program that has no legitimate purpose or business reason for running on the network.

Assessment teams and malicious actors frequently leverage unrestricted code execution in the form of executables, dynamic link libraries (DLLs), HTML applications, and macros (scripts used in office automation documents) [T1059.005] to establish initial access, persistence, and lateral movement. In addition, actors often use scripting languages [T1059] to obscure their actions [T1027.010] and bypass allowlisting—where organizations restrict applications and other forms of code by default and only allow those that are known and trusted. Further, actors may load vulnerable drivers and then exploit the drivers' known vulnerabilities to execute code in the kernel with the highest level of system privileges to completely compromise the device [T1068].

Mitigations

Network defenders

NSA and CISA recommend network defenders implement the recommendations that follow to mitigate the issues identified in this advisory. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST) as well as with the MITRE ATT&CK Enterprise Mitigations and MITRE D3FEND frameworks.

The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.[24]

Mitigate default configurations of software and applications

Table 1: Recommendations for network defenders to mitigate default configurations of software and applications

Misconfiguration	Recommendations for Network Defenders
Default configurations of software and applications	• **Modify the default configuration of applications and appliances before deployment** in a production environment [M1013],[D3-ACH]. Refer to hardening guidelines provided by the vendor and related cybersecurity guidance (e.g., DISA's Security Technical Implementation Guides (STIGs) and configuration guides).[25],[26],[27]
Default configurations of software and applications: Default Credentials	• **Change or disable vendor-supplied default usernames and passwords of services, software, and equipment** when installing or commissioning [CPG 2.A]. When resetting passwords, enforce the use of "strong" passwords (i.e., passwords that are more than 15 characters and random [CPG 2.B]) and follow hardening guidelines provided by the vendor, STIGs, NSA, and/or NIST [M1027],[D3-SPP].[25],[26],[28],[29]

Default service permissions and configuration settings: Insecure Active Directory Certificate Services	• **Ensure the secure configuration of ADCS implementations**. Regularly update and patch the controlling infrastructure (e.g., for CVE-2021-36942), employ monitoring and auditing mechanisms, and implement strong access controls to protect the infrastructure. ○ **If not needed, disable web-enrollment in ADCS servers**. See Microsoft: Uninstall-AdcsWebEnrollment (ADCSDeployment) for guidance.[30] ○ If web enrollment is needed on ADCS servers: ▪ **Enable Extended Protection for Authentication (EPA) for Client Authority Web Enrollment**. This is done by choosing the "Required" option. For guidance, see Microsoft: KB5021989: Extended Protection for Authentication.[31] ▪ **Enable "Require SSL"** on the ADCS server. ○ **Disable NTLM** on all ADCS servers. For guidance, see Microsoft: Network security Restrict NTLM in this domain - Windows Security | Microsoft Learn and Network security Restrict NTLM Incoming NTLM traffic - Windows Security.[32],[33] ○ **Disable SAN for UPN Mapping**. For guidance see, Microsoft: How to disable the SAN for UPN mapping - Windows Server. Instead, smart card authentication can use the altSecurityIdentities attribute for explicit mapping of certificates to accounts more securely.[34] • **Review all permissions on the ADCS templates on applicable servers**. Restrict enrollment rights to only those users or groups that require it. Disable the `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT` flag from templates to prevent users from supplying and editing sensitive security settings within these templates. Enforce manager approval for requested certificates. Remove `FullControl`, `WriteDacl`, and `Write` property permissions from low-privileged groups, such as domain users, to certificate template objects.

Default service permissions and configuration settings: Insecure legacy protocols/services	- **Determine if LLMNR and NetBIOS are required for essential business operations**. ○ If not required, **disable LLMNR and NetBIOS** in local computer security settings or by group policy.
Default service permissions and configuration settings: Insecure SMB service	- **Require SMB signing** for both SMB client and server on all systems.[25] This should prevent certain adversary-in-the-middle and pass-the-hash techniques. For more information on SMB signing, see Microsoft: Overview of Server Message Block Signing. [35] **Note**: Beginning in Microsoft Windows 11 Insider Preview Build 25381, Windows requires SMB signing for all communications.[36]

Mitigate improper separation of user/administrator privilege

Table 2: Recommendations for network defenders to mitigate improper separation of user/administrator privilege

Misconfiguration	Recommendations for Network Defenders
Improper separation of user/administrator privilege: - Excessive account privileges, - Elevated service account permissions, and - Non-essential use of elevated accounts	- **Implement authentication, authorization, and accounting (AAA) systems** [M1018] to limit actions users can perform, and review logs of user actions to detect unauthorized use and abuse. Apply least privilege principles to user accounts and groups allowing only the performance of authorized actions. - **Audit user accounts** and remove those that are inactive or unnecessary on a routine basis [CPG 2.D]. Limit the ability for user accounts to create additional accounts. - **Restrict use of privileged accounts to perform general tasks**, such as accessing emails and browsing the Internet [CPG 2.E],[D3-UAP]. See NSA Cybersecurity Information Sheet (CSI) Defend Privileges and Accounts for more information.[37]

	• **Limit the number of users within the organization with an identity and access management (IAM) role** that has administrator privileges. Strive to reduce all permanent privileged role assignments, and conduct periodic entitlement reviews on IAM users, roles, and policies. • **Implement time-based access for privileged accounts**. For example, the just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model) by setting network-wide policy to automatically disable admin accounts at the Active Directory level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe. In cloud environments, just-in-time elevation is also appropriate and may be implemented using per-session federated claims or privileged access management tools. • **Restrict domain users from being in the local administrator group** on multiple systems. • **Run daemonized applications (services) with non-administrator accounts** when possible. • **Only configure service accounts with the permissions necessary for the services they control to operate**. • **Disable unused services and implement ACLs** to protect services.

Mitigate insufficient internal network monitoring

Table 3: Recommendations for network defenders to mitigate insufficient internal network monitoring

Misconfiguration	Recommendations for Network Defenders
Insufficient internal network monitoring	• **Establish a baseline of applications and services**, and routinely audit their access and use, especially for administrative activity [D3-ANAA]. For instance, administrators should routinely audit the access lists and permissions for of all web applications and services [CPG

	2.O],[M1047]. Look for suspicious accounts, investigate them, and remove accounts and credentials, as appropriate, such as accounts of former staff.[39] - **Establish a baseline that represents an organization's normal traffic activity**, network performance, host application activity, and user behavior; investigate any deviations from that baseline [D3-NTCD],[D3-CSPP],[D3-UBA].[40] - **Use auditing tools capable of detecting privilege and service abuse opportunities** on systems within an enterprise and correct them [M1047]. - **Implement a security information and event management (SIEM) system** to provide log aggregation, correlation, querying, visualization, and alerting from network endpoints, logging systems, endpoint and detection response (EDR) systems and intrusion detection systems (IDS) [CPG 2.T],[D3-NTA].

Mitigate lack of network segmentation

Table 4: Recommendations for network defenders to mitigate lack of network segmentation

Misconfiguration	Recommendations for Network Defenders
Lack of network segmentation	- **Implement next-generation firewalls** to perform deep packet filtering, stateful inspection, and application-level packet inspection [D3-NTF]. Deny or drop improperly formatted traffic that is incongruent with application-specific traffic permitted on the network. This practice limits an actor's ability to abuse allowed application protocols. The practice of allowlisting network applications does not rely on generic ports as filtering criteria, enhancing filtering fidelity. For more information on application-aware defenses, see NSA CSI Segment Networks and Deploy Application-Aware Defenses.[41] - **Engineer network segments to isolate critical systems, functions, and resources** [CPG 2.F],[D3-NI]. Establish physical and logical segmentation controls, such as virtual local area network (VLAN) configurations and

	properly configured access control lists (ACLs) on infrastructure devices [M1030]. These devices should be baselined and audited to prevent access to potentially sensitive systems and information. Leverage properly configured Demilitarized Zones (DMZs) to reduce service exposure to the Internet.[42],[43],[44] • **Implement separate Virtual Private Cloud (VPC) instances** to isolate essential cloud systems. Where possible, implement Virtual Machines (VM) and Network Function Virtualization (NFV) to enable micro-segmentation of networks in virtualized environments and cloud data centers. Employ secure VM firewall configurations in tandem with macro segmentation.

Mitigate poor patch management

Table 5: Recommendations for network defenders to mitigate poor patch management

Misconfiguration	Recommendations for Network Defenders
Poor patch management: Lack of regular patching	• **Ensure organizations implement and maintain an efficient patch management process** that enforces the use of up-to-date, stable versions of OSs, browsers, and software [M1051],[D3-SU].[45] • **Update software regularly by employing patch management** for externally exposed applications, internal enterprise endpoints, and servers. Prioritize patching known exploited vulnerabilities.[2] • **Automate the update process as much as possible** and use vendor-provided updates. Consider using automated patch management tools and software update tools. • Where patching is not possible due to limitations, **segment networks** to limit exposure of the vulnerable system or host.
Poor patch management: Use of unsupported OSs	• **Evaluate the use of unsupported hardware and software and discontinue use** as soon as possible. If

and outdated firmware	discontinuing is not possible, implement additional network protections to mitigate the risk.[45] • **Patch the Basic Input/Output System (BIOS)** and other firmware to prevent exploitation of known vulnerabilities.

Mitigate bypass of system access controls

Table 6: Recommendations for network defenders to mitigate bypass of system access controls

Misconfiguration	Recommendations for Network Defenders
Bypass of system access controls	• **Limit credential overlap across systems** to prevent credential compromise and reduce a malicious actor's ability to move laterally between systems [M1026],[D3-CH]. Implement a method for monitoring non-standard logon events through host log monitoring [CPG 2.G]. • **Implement an effective and routine patch management process**. Mitigate PtH techniques by applying patch KB2871997 to Windows 7 and newer versions to limit default access of accounts in the local administrator group [M1051],[D3-SU].[46] • **Enable the PtH mitigations to apply User Account Control (UAC) restrictions** to local accounts upon network logon [M1052],[D3-UAP]. • **Deny domain users the ability to be in the local administrator group** on multiple systems [M1018],[D3-UAP]. • **Limit workstation-to-workstation communications**. All workstation communications should occur through a server to prevent lateral movement [M1018],[D3-UAP]. • **Use privileged accounts only on systems requiring those privileges** [M1018],[D3-UAP]. Consider using dedicated Privileged Access Workstations for privileged accounts to better isolate and protect them.[37]

Mitigate weak or misconfigured MFA methods

Table 7: Recommendations for network defenders to mitigate weak or misconfigured MFA methods

Misconfiguration	Recommendations for Network Defenders
Weak or misconfigured MFA methods: Misconfigured smart cards or tokens	- In Windows environments: ○ **Disable the use of New Technology LAN Manager (NTLM) and other legacy authentication protocols** that are susceptible to PtH due to their use of password hashes [M1032],[D3-MFA]. For guidance, see Microsoft: Network security Restrict NTLM in this domain - Windows Security | Microsoft Learn and Network security Restrict NTLM Incoming NTLM traffic - Windows Security.[32],[33] ○ **Use built-in functionality via Windows Hello for Business or Group Policy Objects (GPOs) to regularly re-randomize password hashes** associated with smartcard-required accounts. Ensure that the hashes are changed at least as often as organizational policy requires passwords to be changed [M1027],[D3-CRO]. Prioritize upgrading any environments that cannot utilize this built-in functionality. - As a longer-term effort, **implement cloud-primary authentication solution using modern open standards**. See CISA's Secure Cloud Business Applications (SCuBA) Hybrid Identity Solutions Architecture for more information.[47] **Note:** this document is part of CISA's Secure Cloud Business Applications (SCuBA) project, which provides guidance for FCEB agencies to secure their cloud business application environments and to protect federal information that is created, accessed, shared, and stored in those environments. Although tailored to FCEB agencies, the project's guidance is applicable to all organizations.[48]

Weak or misconfigured MFA methods: Lack of phishing-resistant MFA	- **Enforce phishing-resistant MFA universally** for access to sensitive data and on as many other resources and services as possible [CPG 2.H].[3],[49]

Mitigate insufficient ACLs on network shares and services

Table 8: Recommendations for network defenders to mitigate insufficient ACLs on network shares and services

Misconfiguration	Recommendations for Network Defenders
Insufficient ACLs on network shares and services	- **Implement secure configurations for all storage devices** and network shares that grant access to authorized users only. - **Apply the principal of least privilege** to important information resources to reduce risk of unauthorized data access and manipulation. - **Apply restrictive permissions to files and directories**, and prevent adversaries from modifying ACLs [M1022],[D3-LFP]. - **Set restrictive permissions on files and folders containing sensitive private keys** to prevent unintended access [M1022],[D3-LFP]. - **Enable the Windows Group Policy security setting, "Do Not Allow Anonymous Enumeration of Security Account Manager (SAM) Accounts and Shares,"** to limit users who can enumerate network shares.

Mitigate poor credential hygiene

Table 9: Recommendations for network defenders to mitigate poor credential hygiene

Misconfiguration	Recommendations for Network Defenders
Poor credential hygiene: easily	- **Follow National Institute of Standards and Technologies (NIST) guidelines when creating**

crackable passwords	**password policies** to enforce use of “strong” passwords that cannot be cracked [M1027],[D3-SPP].[29] Consider using password managers to generate and store passwords. • **Do not reuse local administrator account passwords across systems**. Ensure that passwords are “strong” and unique [CPG 2.B],[M1027],[D3-SPP]. • **Use “strong” passphrases for private keys** to make cracking resource intensive. Do not store credentials within the registry in Windows systems. Establish an organizational policy that prohibits password storage in files. • **Ensure adequate password length (ideally 25+ characters) and complexity requirements for Windows service accounts** and implement passwords with periodic expiration on these accounts [CPG 2.B],[M1027],[D3-SPP]. Use Managed Service Accounts, when possible, to manage service account passwords automatically.
Poor credential hygiene: cleartext password disclosure	• **Implement a review process for files and systems to look for cleartext account credentials**. When credentials are found, remove, change, or encrypt them [D3-FE]. Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, protected health information) or credentials are stored. Weigh the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is of significant concern, technical controls, policy, and user training may prevent storage of credentials in improper locations. • **Store hashed passwords using Committee on National Security Systems Policy (CNSSP)-15 and Commercial National Security Algorithm Suite (CNSA) approved algorithms**.[50],[51]

	• **Consider using group Managed Service Accounts (gMSAs) or third-party software** to implement secure password-storage applications.

Mitigate unrestricted code execution

Table 10: Recommendations for network defenders to mitigate unrestricted code execution

Misconfiguration	Recommendations for Network Defenders
Unrestricted code execution	• **Enable system settings that prevent the ability to run applications downloaded from untrusted sources**.[52] • **Use application control tools that restrict program execution by default, also known as allowlisting** [D3-EAL]. Ensure that the tools examine digital signatures and other key attributes, rather than just relying on filenames, especially since malware often attempts to masquerade as common Operating System (OS) utilities [M1038]. Explicitly allow certain `.exe` files to run, while blocking all others by default. • **Block or prevent the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode**. Validate driver block rules in audit mode to ensure stability prior to production deployment [D3-OSM]. • **Constrain scripting languages to prevent malicious activities, audit script logs, and restrict scripting languages** that are not used in the environment [D3-SEA]. See joint Cybersecurity Information Sheet: Keeping PowerShell: Security Measures to Use and Embrace.[53] • **Use read-only containers and minimal images**, when possible, to prevent the running of commands. • **Regularly analyze border and host-level protections, including spam-filtering capabilities**, to ensure their continued effectiveness in blocking the delivery and execution of malware [D3-MA]. Assess whether HTML Application (HTA) files are used for business purposes in your environment; if HTAs are not used, remap the default

	program for opening them from `mshta.exe` to `notepad.exe`.

Software manufacturers

NSA and CISA recommend software manufacturers implement the recommendations in Table 11 to reduce the prevalence of misconfigurations identified in this advisory. These mitigations align with tactics provided in joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default. NSA and CISA strongly encourage software manufacturers apply these recommendations to ensure their products are secure "out of the box" and do not require customers to spend additional resources making configuration changes, performing monitoring, and conducting routine updates to keep their systems secure.[1]

Table 11: Recommendations for software manufacturers to mitigate identified misconfigurations

Misconfiguration	Recommendations for Software Manufacturers
Default configurations of software and applications	• **Embed security controls into product architecture from the start of development and throughout the entire SDLC** by following best practices in NIST's Secure Software Development Framework (SSDF), SP 800-218.[54] • **Provide software with security features enabled "out of the box" and accompanied with "loosening" guides** instead of hardening guides. "Loosening" guides should explain the business risk of decisions in plain, understandable language.
Default configurations of software and applications: Default credentials	• **Eliminate default passwords**: Do not provide software with default passwords that are universally shared. To eliminate default passwords, require administrators to set a "strong" password [CPG 2.B] during installation and configuration.

Default configurations of software and applications: Default service permissions and configuration settings	• **Consider the user experience consequences of security settings**: Each new setting increases the cognitive burden on end users and should be assessed in conjunction with the business benefit it derives. Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default. When configuration is necessary, the default option should be broadly secure against common threats.
Improper separation of user/administrator privilege: • Excessive account privileges, • Elevated service account permissions, and • Non-essential use of elevated accounts	• **Design products so that the compromise of a single security control does not result in compromise of the entire system**. For example, ensuring that user privileges are narrowly provisioned by default and ACLs are employed can reduce the impact of a compromised account. Also, software sandboxing techniques can quarantine a vulnerability to limit compromise of an entire application. • **Automatically generate reports for:** ○ **Administrators of inactive accounts.** Prompt administrators to set a maximum inactive time and automatically suspend accounts that exceed that threshold. ○ **Administrators of accounts with administrator privileges** and suggest ways to reduce privilege sprawl. • **Automatically alert administrators of infrequently used services** and provide recommendations for disabling them or implementing ACLs.
Insufficient internal network monitoring	• **Provide high-quality audit logs to customers at no extra charge**. Audit logs are crucial for detecting and escalating potential security incidents. They are also crucial during an investigation of a suspected or confirmed security

	incident. Consider best practices such as providing easy integration with a security information and event management (SIEM) system with application programming interface (API) access that uses coordinated universal time (UTC), standard time zone formatting, and robust documentation techniques.
Lack of network segmentation	• **Ensure products are compatible with and tested in segmented network environments**.
Poor patch management: Lack of regular patching	• **Take steps to eliminate entire classes of vulnerabilities by embedding security controls into product architecture from the start of development and throughout the SDLC by following best practices in NIST's SSDF**, SP 800-218.[54] Pay special attention to: ○ **Following secure coding practices** [SSDF PW 5.1]. Use memory-safe programming languages where possible, parametrized queries, and web template languages. ○ **Conducting code reviews** [SSDF PW 7.2, RV 1.2] against peer coding standards, checking for backdoors, malicious content, and logic flaws. ○ **Testing code to identify vulnerabilities** and verify compliance with security requirements [SSDF PW 8.2]. • **Ensure that published CVEs include root cause or common weakness enumeration (CWE)** to enable industry-wide analysis of software security design flaws.
Poor patch management: Use of unsupported operating OSs and outdated firmware	• **Communicate the business risk of using unsupported OSs and firmware** in plain, understandable language.

Bypass of system access controls	• **Provide sufficient detail in audit records to detect bypass of system controls** and queries to monitor audit logs for traces of such suspicious activity (e.g., for when an essential step of an authentication or authorization flow is missing).
Weak or Misconfigured MFA Methods: Misconfigured Smart Cards or Tokens	• **Fully support MFA for all users**, making MFA the default rather than an opt-in feature. Utilize threat modeling for authentication assertions and alternate credentials to examine how they could be abused to bypass MFA requirements.
Weak or Misconfigured MFA Methods: Lack of phishing-resistant MFA	• **Mandate MFA, ideally phishing-resistant, for privileged users** and make MFA a default rather than an opt-in feature.[3]
Insufficient ACL on network shares and services	• **Enforce use of ACLs** with default ACLs only allowing the minimum access needed, along with easy-to-use tools to regularly audit and adjust ACLs to the minimum access needed.
Poor credential hygiene: easily crackable passwords	• **Allow administrators to configure a password policy consistent with NIST's guidelines**—do not require counterproductive restrictions such as enforcing character types or the periodic rotation of passwords.[29] • **Allow users to use password managers** to effortlessly generate and use secure, random passwords within products.
Poor credential hygiene: cleartext password disclosure	• **Salt and hash passwords using a secure hashing algorithm** with high computational cost to make brute force cracking more difficult.
Unrestricted code execution	• **Support execution controls** within operating systems and applications "out of the box" by default at no extra charge for all customers, to limit malicious actors' ability to abuse functionality

	or launch unusual applications without administrator or informed user approval.

Validate security controls

In addition to applying mitigations, NSA and CISA recommend exercising, testing, and validating your organization’s security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. NSA and CISA recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 12–Table 21).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies’ performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and NSA recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Learn from history

The misconfigurations described above are all too common in assessments and the techniques listed are standard ones leveraged by multiple malicious actors, resulting in numerous real network compromises. Learn from the weaknesses of others and implement the mitigations above properly to protect the network, its sensitive information, and critical missions.

Works cited

[1] Joint Guide: Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (2023), https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf

[2] CISA, Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[3] CISA, Implementing Phishing-Resistant MFA, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[4] MITRE, ATT&CK for Enterprise, https://attack.mitre.org/versions/v13/matrices/enterprise/

[5] MITRE, D3FEND, https://d3fend.mitre.org/

[6] CISA, Best Practices for MITRE ATT&CK Mapping, https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping

[7] CISA, Decider Tool, https://github.com/cisagov/Decider/

[8] CISA, Cyber Assessment Fact Sheet, https://www.cisa.gov/sites/default/files/publications/VM_Assessments_Fact_Sheet_RVA_508C.pdf

[9] Joint CSA: Weak Security Controls and Practices Routinely Exploited for Initial Access, https://media.defense.gov/2022/May/17/2002998718/-1/-1/0/CSA_WEAK_SECURITY_CONTROLS_PRACTICES_EXPLOITED_FOR_INITIAL_ACCESS.PDF

[10] Microsoft KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS), https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

[11] Raj Chandel, Domain Escalation: PetitPotam NTLM Relay to ADCS Endpoints, https://www.hackingarticles.in/domain-escalation-petitpotam-ntlm-relay-to-adcs-endpoints/

[12] SpecterOps - Will Schroeder, Certified Pre-Owned, https://posts.specterops.io/certified-pre-owned-d95910965cd2

[13] CISA, CSA: CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a

[14] Joint CSA: Threat Actors Exploit Progress Telerik Vulnerabilities in Multiple U.S. Government IIS Servers. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-074a

[15] Joint CSA: Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a

[16] Joint CSA: Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-228a

[17] Microsoft, How to verify that MS17-010 is installed, https://support.microsoft.com/en-us/topic/how-to-verify-that-ms17-010-is-installed-f55d3f13-7a9c-688c-260b-477d0ec9f2c8

[18] Microsoft, Microsoft Security Bulletin MS08-067 – Critical Vulnerability in Server Service Could Allow Remote Code Execution (958644), https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

[19] Joint CSA: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-277a

[20] CISA, Malware Analysis Report: 10365227.r1.v1, https://www.cisa.gov/sites/default/files/2023-06/mar-10365227.r1.v1.clear_.pdf

[21] Joint CSA: #StopRansomware: BianLian Ransomware Group. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

[22] CISA Analysis Report: FiveHands Ransomware. https://www.cisa.gov/news-events/analysis-reports/ar21-126a

[23] Snaffler, https://github.com/SnaffCon/Snaffler

[24] CISA, Cross-Sector Cybersecurity Performance Goals, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[25] Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs), https://public.cyber.mil/stigs/

[26] NSA, Network Infrastructure Security Guide, https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

[27] NSA, Actively Manage Systems and Configurations, https://media.defense.gov/2019/Sep/09/2002180326/-1/-1/0/Actively%20Manage%20Systems%20and%20Configurations.docx%20-%20Copy.pdf

[28] NSA, Cybersecurity Advisories & Guidance, https://www.nsa.gov/cybersecurity-guidance

[29] National Institute of Standards and Technologies (NIST), NIST SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management, https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final

[30] Microsoft, Uninstall-AdcsWebEnrollment, https://learn.microsoft.com/en-us/powershell/module/adcsdeployment/uninstall-adcswebenrollment

[31] Microsoft, KB5021989: Extended Protection for Authentication, https://support.microsoft.com/en-au/topic/kb5021989-extended-protection-for-authentication-1b6ea84d-377b-4677-a0b8-af74efbb243f

[32] Microsoft, Network security: Restrict NTLM: NTLM authentication in this domain, https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain

[33] Microsoft, Network security: Restrict NTLM: Incoming NTLM traffic, https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-incoming-ntlm-traffic

[34] Microsoft, How to disable the Subject Alternative Name for UPN mapping, https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/disable-subject-alternative-name-upn-mapping

[35] Microsoft, Overview of Server Message Block signing, https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

[36] Microsoft, SMB signing required by default in Windows Insider, https://aka.ms/SmbSigningRequired

[37] NSA, Defend Privileges and Accounts, https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/Defend%20Privileges%20and%20Accounts%20-%20Copy.pdf

[38] NSA, Advancing Zero Trust Maturity Throughout the User Pillar, https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF

[39] NSA, Continuously Hunt for Network Intrusions, https://media.defense.gov/2019/Sep/09/2002180360/-1/-1/0/Continuously%20Hunt%20for%20Network%20Intrusions%20-%20Copy.pdf

[40] Joint CSI: Detect and Prevent Web Shell Malware, https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF

[41] NSA, Segment Networks and Deploy Application-aware Defenses, https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf

[42] Joint CSA: NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF

[43] NSA, Stop Malicious Cyber Activity Against Connected Operational Technology, https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/0/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF

[44] NSA, Performing Out-of-Band Network Management, https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT20200911.PDF

[45] NSA, Update and Upgrade Software Immediately, https://media.defense.gov/2019/Sep/09/2002180319/-1/-1/0/Update%20and%20Upgrade%20Software%20Immediately.docx%20-%20Copy.pdf

[46] Microsoft, Microsoft Security Advisory 2871997: Update to Improve Credentials Protection and Management, https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997

[47] CISA, Secure Cloud Business Applications Hybrid Identity Solutions Architecture, https://www.cisa.gov/sites/default/files/2023-03/csso-scuba-guidance_document-hybrid_identity_solutions_architecture-2023.03.22-final.pdf

[48] CISA, Secure Cloud Business Applications (SCuBA) Project, https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[49] NSA, Transition to Multi-factor Authentication, https://media.defense.gov/2019/Sep/09/2002180346/-1/-1/0/Transition%20to%20Multi-factor%20Authentication%20-%20Copy.pdf

[50] Committee on National Security Systems (CNSS), CNSS Policy 15, https://www.cnss.gov/CNSS/issuances/Policies.cfm

[51] NSA, NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

[52] NSA, Enforce Signed Software Execution Policies, https://media.defense.gov/2019/Sep/09/2002180334/-1/-1/0/Enforce%20Signed%20Software%20Execution%20Policies%20-%20Copy.pdf

[53] Joint CSI: Keeping PowerShell: Security Measures to Use and Embrace, https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/0/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF

[54] NIST, NIST SP 800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, https://csrc.nist.gov/publications/detail/sp/800-218/final

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademarks

Active Directory, Microsoft, and Windows are registered trademarks of Microsoft Corporation.
MITRE ATT&CK is registered trademark and MITRE D3FEND is a trademark of The MITRE Corporation.
SoftPerfect is a registered trademark of SoftPerfect Proprietary Limited Company.
Telerik is a registered trademark of Progress Software Corporation.
VMware is a registered trademark of VMWare, Inc.
Zimbra is a registered trademark of Synacor, Inc.

Purpose

This document was developed in furtherance of the authoring cybersecurity organizations’ missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

To report suspicious activity contact CISA’s 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Appendix: MITRE ATT&CK tactics and techniques

See Table 12–Table 21 for all referenced threat actor tactics and techniques in this advisory.

Table 12: ATT&CK Techniques for Enterprise – Reconnaissance

Technique Title	ID	Use
Active Scanning: Vulnerability Scanning	T1595.002	Malicious actors scan victims for vulnerabilities that be exploited for initial access.
Gather Victim Host Information	T1592	Malicious actors gather information on victim client configurations and/or vulnerabilities through vulnerabilities scans and searching the web.
Gather Victim Identity Information: Credentials	T1589.001	Malicious actors find default credentials through searching the web.
Phishing for Information	T1598	Malicious actors masquerade as IT staff and convince a target user to provide their MFA code over the phone to gain access to email and other organizational resources.

Table 13: ATT&CK Techniques for Enterprise – Initial Access

Technique Title	ID	Use
External Remote Services	T1133	Malicious actors use default credentials for VPN access to internal networks.

Technique Title	ID	Use
Valid Accounts: Default Accounts	T1078.001	Malicious actors gain authenticated access to devices by finding default credentials through searching the web. Malicious actors use default credentials for VPN access to internal networks, and default administrative credentials to gain access to web applications and databases.
Exploit Public-Facing Application	T1190	Malicious actors exploit CVEs in Telerik UI, VM Horizon, Zimbra Collaboration Suite, and other applications for initial access to victim organizations.
Phishing	T1566	Malicious actors gain initial access to systems by phishing to entice end users to download and execute malicious payloads.
Trust Relationship	T1199	Malicious actors gain access to OT networks despite prior assurance that the networks were fully air gapped, with no possible connection to the IT network, by finding special purpose, forgotten, or even accidental network connections.

Table 14: ATT&CK Techniques for Enterprise – Execution

Technique Title	ID	Use
Software Deployment Tools	T1072	Malicious actors use default or captured credentials on software deployment tools to execute code and move laterally.

Technique Title	ID	Use
User Execution	T1204	Malicious actors gain initial access to systems by phishing to entice end users to download and execute malicious payloads or to run code on their workstations.
Command and Scripting Interpreter	T1059	Malicious actors use scripting languages to obscure their actions and bypass allowlisting.
Command and Scripting Interpreter: Visual Basic	T1059.005	Malicious actors use macros for initial access, persistence, and lateral movement.

Table 15: ATT&CK Techniques for Enterprise – Persistence

Technique Title	ID	Use
Account Manipulation	T1098	Malicious actors reset built-in administrative accounts via predictable, forgotten password questions.

Table 16: ATT&CK Techniques for Enterprise – Privilege Escalation

Technique Title	ID	Use
Valid Accounts	T1078	Malicious actors analyze topical and nested Active Directory groups to find privileged accounts to target.
Valid Accounts: Domain Accounts	T1078.002	Malicious actors obtain loaded domain credentials from printers and scanners and use them to move laterally from the network device.

Exploitation for Privilege Escalation	T1068	Malicious actors load vulnerable drivers and then exploit their known vulnerabilities to execute code in the kernel with the highest level of system privileges to completely compromise the device.

Table 17: ATT&CK Techniques for Enterprise – Defense Evasion

Technique Title	ID	Use
Obfuscated Files or Information: Command Obfuscation	T1027.010	Malicious actors often use scripting languages to obscure their actions.

Table 18: ATT&CK Techniques for Enterprise – Credential Access

Technique Title	ID	Use
Adversary-in-the-Middle	T1557	Malicious actors force a device to communicate through actor-controlled systems, so they can collect information or perform additional actions.
Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	T1557.001	Malicious actors execute spoofing, poisoning, and relay techniques if Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS), and Server Message Block (SMB) services are enabled in a network.
Brute Force: Password Cracking	T1110.002	Malicious actors capture user hashes and leverage dictionary wordlists and rulesets to extract cleartext passwords.

Technique Title	ID	Use
Credentials from Password Stores	T1555	Malicious actors gain access to and crack credentials from PFX stores, enabling elevation of privileges and lateral movement within networks.
Multi-Factor Authentication Interception	T1111	Malicious actors can obtain password hashes for accounts enabled for MFA with smart codes or tokens and use the hash via PtH techniques.
Multi-Factor Authentication Request Generation	T1621	Malicious actors use "push bombing" against non-phishing resistant MFA to induce "MFA fatigue" in victims, gaining access to MFA authentication credentials or bypassing MFA, and accessing the MFA-protected system.
Steal Application Access Token	T1528	Malicious actors can steal administrator account credentials and the authentication token generated by Active Directory when the account is logged into a compromised host.
Steal or Forge Authentication Certificates	T1649	Unauthenticated malicious actors coerce an ADCS server to authenticate to an actor-controlled server, and then relay that authentication to the web certificate enrollment application to obtain a trusted illegitimate certificate.
Steal or Forge Kerberos Tickets: Golden Ticket	T1558.001	Malicious actors who have obtained authentication certificates can use the certificate for Active Directory authentication to obtain a Kerberos TGT.

Technique Title	ID	Use
Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	Malicious actors obtain and abuse valid Kerberos TGTs to elevate privileges and laterally move throughout an organization's network.
Unsecured Credentials: Credentials in Files	T1552.001	Malicious actors find cleartext credentials that organizations or individual users store in spreadsheets, configuration files, and other documents.

Table 19: ATT&CK Techniques for Enterprise – Discovery

Technique Title	ID	Use
Account Discovery	T1087	Malicious actors with valid domain credentials enumerate the AD to discover elevated accounts and where they are used.
File and Directory Discovery	T1083	Malicious actors use commands, such as `net share`, open source tools, such as SoftPerfect Network Scanner, or custom malware, such as CovalentStealer to discover and categorize files. Malicious actors search for text files, spreadsheets, documents, and configuration files in hopes of obtaining desired information, such as cleartext passwords.
Network Share Discovery	T1135	Malicious actors use commands, such as `net share`, open source tools, such as SoftPerfect Network Scanner, or custom

Technique Title	ID	Use
		malware, such as CovalentStealer, to look for shared folders and drives.

Table 20: ATT&CK Techniques for Enterprise – Lateral Movement

Technique Title	ID	Use
Exploitation of Remote Services	T1210	Malicious actors can exploit OS and firmware vulnerabilities to gain unauthorized network access, compromise sensitive data, and disrupt operations.
Remote Services: SMB/Windows Admin Shares	T1021.002	If SMB signing is not enforced, malicious actors can use name resolution poisoning to access remote systems.
Use Alternate Authentication Material: Application Access Token	T1550.001	Malicious actors with stolen administrator account credentials and AD authentication tokens can use them to operate with elevated permissions throughout the domain.
Use Alternate Authentication Material: Pass the Hash	T1550.002	Malicious actors collect hashes in a network and authenticate as a user without having access to the user's cleartext password.

Table 21: ATT&CK Techniques for Enterprise – Collection

Technique Title	ID	Use
Data from Network Shared Drive	T1039	Malicious actors find sensitive information on network shares that could facilitate

Technique Title	ID	Use
		follow-on activity or provide opportunities for extortion.