



THREAT INSIGHTS 2023

ADVERSARY TRENDS AND
RECENT VULNERABILITIES

VOLUME IV

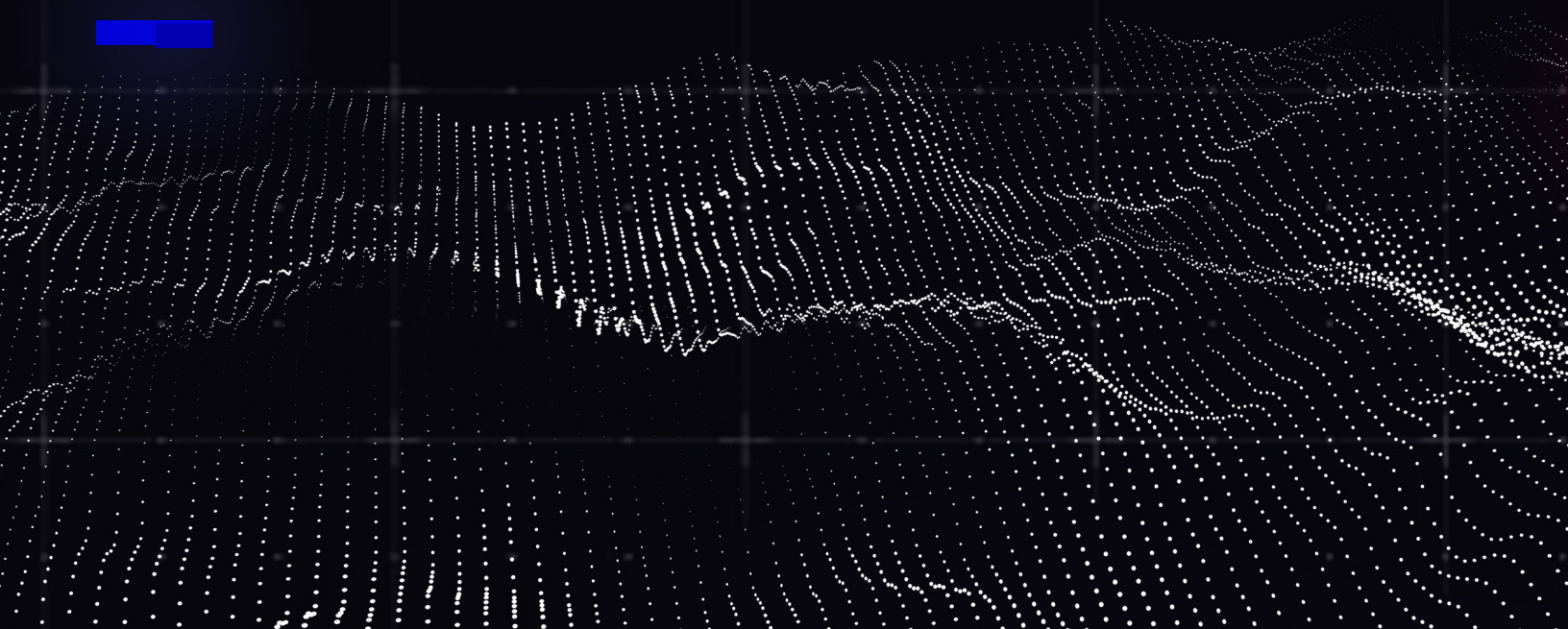


TABLE OF CONTENTS

Executive Summary	3	Notable CVEs This Quarter	9
Key Insights	3	Vulnerabilities CVE-2023-3519: Analysis and Mitigation Strategies in Citrix Products	9
Introduction.....	4	CVE-2023-2868: Critical Vulnerability in Barracuda Email Security Gateway Products	11
Threat 1: BianLan	5	CVE-2023-20198 and CVE-2023-20273: Dual Critical Vulnerabilities in Cisco IOS XE Products.....	12
Overview of BianLan Operations and TTPsRecent Operations	5	Report Recommendations	14
Insights and Strategic Analysis	5	References	15
Mitigation Strategies and Best Practice.....	6	About Adlumin	16
Conclusion.....	6		
Threat 2: Medusa Group	7		
Overview of Medusa Operations and TTPs.....	7		
Mitigation Strategies	8		
Conclusion.....	8		

AUTHORS

ADLUMIN'S THREAT RESEARCH TEAM

Adlumin's Threat Research Team is the innovator behind Adlumin's comprehensive threat hunting to improve visibility, reduce complexity, and manage risk. The team proactively searches for cyber threats lurking undetected in your network environment. They dig deep to identify non-remediated threats and other malicious activities to reinforce security defenses.

EXECUTIVE SUMMARY

Adlumin's Winter 2023 Cybersecurity Insights Report highlights significant trends and developments in the threats, vulnerabilities, and cyberattacks faced by U.S. industries and sectors observed from September to November 2023 by Adlumin's Threat Research Team.

This report provides an overview of the current cyber threat landscape, focusing on two trending threat actors and three of the most pressing vulnerabilities discovered in the third quarter of 2023. Below is a list of the main findings:

KEY INSIGHTS



THREAT ACTORS

- BianLian, once only known for ransomware, has broadened its approach to a more versatile cybercriminal strategy. This includes advanced persistent threats (APTs), customized malware, and zero-day exploit utilization.
- Medusa Ransomware has been involved in a wide number of attacks on schools, hospitals, and financial institutions, recently claiming to have struck Toyota Financial.
 - Medusa Ransomware typically gains access to the victim network either through spear-phishing or by leveraging vulnerable RDP configurations and brute-forcing passwords



VULNERABILITIES

- CVE-2023-3519 represents a critical vulnerability in certain Citrix products, posing significant risks to enterprise networks and data security.
 - CVE-2023-3519 arises due to Improper Control of Generation of the Code ('Code Injection') CWE-94 [1]; this flaw allows attackers to execute arbitrary code remotely, gain system privileges, and access sensitive data.
- CVE-2023-2868 is a critical remote command injection vulnerability found in Barracuda Email Security Gateway (ESG) appliances, affecting versions 5.1.3.001 to 9.2.0.006.
 - CVE-2023-2868 has been actively exploited by threat actors, leading to notable compromises such as the attack on the Australian Capital Territory government.
- CVE-2023-20198 allows an attacker to gain initial access by issuing a privilege 15 command to create a local user and password combination, thus obtaining normal user access^[3].

INTRODUCTION

Operating amidst the ever-present danger of cyberattacks has become the norm for businesses of all sizes. Reports from the Information Systems Audit and Control Association (ISACA) suggest that approximately 76% of organizations were targeted by ransomware last year, highlighting the prevalent threat^[1].

At Adlumin, our daily operations involve vigilant observation and tracking of these concerning patterns – examining cyber threats, Tactics, Techniques, and Procedures (TTPs), pinpointing the targeted industries and threat actors, discovering fresh avenues for infiltration, and understanding the methods, tactics, and procedures employed by these threat actors.

This quarter’s cyber threat report emphasizes the ongoing risks and vulnerabilities we have identified as potentially impacting businesses, mainly concentrating on probable threats within the mid-market segment.

TRENDING CYBERTHREATS THIS QUARTER

We begin by highlighting the significant dangers that mid-sized businesses dealt with in September, October and November 2023. This includes looking at cybercriminals, their operations, and their usual patterns.



Threat 1: BianLian

Overview of BianLian Operations and TTPs

BianLian, once only known for ransomware, has broadened its approach to a more versatile cybercriminal strategy. This includes advanced persistent threats (APTs), customized malware, and zero-day exploit utilization. Key features of their modus operandi involve:

- **Custom Malware Deployment:** BianLian's malware is known for its modularity and evasion capabilities against conventional antivirus systems.
- **Targeted Phishing:** Spear-phishing allows the threat actors to leverage social engineering to extract sensitive information.
- **Zero-Day Exploitation:** A penchant for exploiting unknown software vulnerabilities, indicating significant technical acumen.

Recent Operations

BianLian's latest campaigns, particularly against a major financial institution, involved deploying a custom backdoor for data exfiltration, underscoring their focus on corporate espionage.

Impact on Cybersecurity

BianLian poses a substantial threat due to the following:

- **Rapid Evolution:** The group's swift adaptation and tactical refinement are concerning.
- **Target Diversity:** BianLian poses risks across various sectors not confined to a specific industry.
- **Sophistication:** The group's technical prowess suggests the involvement of seasoned cybercriminals.

Parallels with Other Cyber Threats

BianLian shares similarities with APT29 and the North Korea Lazarus Group in methodical target selection, preference for stealth, and bespoke tool utilization.

Defenses and Mitigations

A multifaceted defense strategy is essential, including:

1. **Enhanced Detection and Response:** Implement behavior-based analytics for early detection.
2. **Regular Software Patching:** Crucial for thwarting exploitation attempts.
3. **Employee Training:** Essential to mitigate phishing risks.
4. **Network Segmentation:** Limits attack spread within an organization.
5. **Incident Response Planning:** Key for rapid reaction and recovery.

BianLian: Insights and Strategic Analysis

BianLian's malware demonstrates advanced technical proficiency, often polymorphic and equipped with anti-detection features. The group utilizes encryption and obfuscation, which challenges forensic analysis.

Intrusion Techniques

BianLian's methods include zero-day vulnerability exploitation and supply chain compromises, signifying their extensive technical knowledge and information networks.

BianLian uses advanced lateral movement strategies and complex persistence mechanisms to ensure long-term access to compromised networks.

BianLian's actions are multifaceted threats involving significant data breaches and corporate espionage,

hinting at possible state-sponsored activities or alliances for competitive gains.

BianLian parallels other hacking groups, such as APT28 and DarkHotel, in zero-day exploit utilization and espionage-focused malware development.

Unfolding an Attack

Adlumin's Incident Response team responded to a BianLian attack that appeared to be a case of two BianLian affiliates infiltrating the same victim.



At first, reacting to and engaging with an assault by BianLian led to the transmission of ransom messages specifically aimed at the IT personnel. The probable entry point was through credential stuffing on a remote access platform utilized by the target.

During our investigation we found additional compromised hosts that had been silently exfiltrating data since before Adlumin had even been deployed in the network. The exfiltration was being done with open-source backup tools and there were no traces of remote access tools left behind by the attacker.

The attackers organized their data extraction operations and patiently waited to amass sufficient data for a ransom attempt. However, a less skilled BianLian affiliate rushed in and hastily tried to initiate a ransom after encountering difficulties while navigating the network. BianLian affiliates often overlap in targeting and will pursue a ransom even without firmly establishing themselves within the victim's network.

Mitigation Strategies and Best Practices

Effective countermeasures include:

1. **Advanced Threat Hunting:** To identify specific compromise indicators.
2. **Endpoint Detection and Response (EDR):** For detecting and responding to BianLian's tactics.
3. **Zero Trust Architecture:** To minimize breach impacts.
4. **Threat Intelligence Sharing:** To enhance early detection and prevention.
5. **Regular Security Audits and Penetration Testing:** To identify and mitigate potential vulnerabilities. Strategic Implications and Mitigation

Strategic Implications and Mitigation

- **Evasion Techniques:** Necessitates sophisticated detection systems.
- **Targeted Nature:** Calls for industry-specific cybersecurity strategies.
- **Advanced Persistent Threat:** Highlights the need for continuous monitoring and regular security audits.

Conclusion

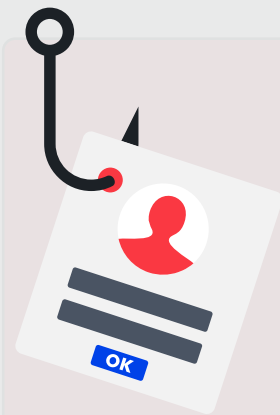
BianLian represents a sophisticated and evolving cyber threat, necessitating continuous monitoring and adaptive cybersecurity measures for effective risk mitigation. Understanding their tactics and implementing proactive defenses is vital for organizational protection.

Threat 2: Medusa Group

The Medusa Group stands out as a sophisticated and formidable adversary in the rapidly evolving landscape of cybersecurity threats. This section of the report analyzes the group's recent activities, technical prowess, and operational strategies and suggests effective mitigation strategies. The assessment is based on the latest intelligence, incident reports, and Adlumin's cybersecurity research.

Overview of Medusa's Operations and TTPs

Believed to be using a ransomware-as-a-Service model ^[1], the Medusa Ransomware has been involved in a wide number of attacks on schools, hospitals, and financial institutions, recently claiming to have struck Toyota Financial ^[2].



The threat actors typically gain access to the victim network through spear-phishing or leveraging vulnerable RDP configurations and brute-forcing passwords ^[2&3].

Following initial access, actors will perform reconnaissance within the network before encrypting and exfiltrating data ^[1&5]. BianLian uses advanced lateral movement strategies and complex persistence mechanisms to ensure long-term access to compromised networks.

Social Engineering and Spear Phishing

Medusa's reliance on social engineering is evident in its spear-phishing campaigns. Medusa Locker leveraged the widespread interest surrounding the COVID-19 pandemic to launch attacks, gaining entry into networks via phishing campaigns in which the malware is attached to emails ^[11].

Network Propagation and Lateral Movement

Once inside a network, Medusa operators quickly establish persistence through connected webshells or by creating a new administrative user account ^[3]. The group also disables antivirus and deletes shadow copies, making detecting or restoring encrypted data harder ^[2&4]. Medusa operators are also known to reboot the computer into Safe Mode to make it easier to bypass defenses ^[6]. While they establish persistence rather quickly, the attackers have been known to have an extended stay in the network, taking the better part of a year to go from initial entry to ransomware execution ^[5].

Encryption and Exfiltration Techniques

The group's skill in concealing their activities is notable. In several instances, they have used advanced encryption methods to exfiltrate data, challenging detection by standard network monitoring tools.

Medusa ransomware uses the BCrypt library to encrypt data on the victim's machine before deleting shadow copies. Files are encrypted with AES-256 encryption ^[7].

Recent Exploits and Operations

Medusa keeps a live feed on its blog showing a list of new activities. Recently, they have claimed responsibility for a

data breach at Toyota Financial and Community Hospital in Tallahassee ^[1]. The group is widely known for the attack and release of data on the Minneapolis Public School Systems, where they released psychological reports and abuse allegations related to students ^[8]. Recently, Medusa has claimed to have breached Moneris Solutions. However, the company has responded that no ransom request was made as they had prevented access to critical data ^[9].

Strategic Overview

Medusa's operations suggest a strategy focused on long-term penetration using RaaS toolkits, data harvesting, and financial gain. Their selection process appears highly methodical, indicative of extensive planning and reconnaissance.

Mitigation Strategies

Enhanced Email Filtering

To counter spear-phishing attacks, organizations should implement advanced email filtering solutions. Many standard email providers, such as Office365 and Google Suite, offer advanced Machine Learning and AI-driven email filtering and protection ^[12,13].

Regular Software Updates and Patch Management

Maintaining updated software, particularly applying security patches promptly, is crucial. Medusa's usage of existing known exploits, as shown in attacks against Windak Group and Karman Chand Thapar & Bros, reflects the need to maintain updated software in the context of Medusa group's exploitation tactics ^[14].

Network Segmentation

Segmenting networks can limit the extent of lateral movement. The National Institute of Science and

Technology (NIST) provides a comprehensive approach to effective segmentation in NIST SP 800-215 ^[15].

Additionally, consult CISA's January 2022 publication on Layering Network Security Through Segmentation ^[16].

Employee Training

Security training is essential for empowering employees with the knowledge and skills needed to identify and respond to potential threats, thereby mitigating the risk of data breaches and unauthorized access—a critical aspect often overlooked, as emphasized in the words: “Failure to give attention to the area of security training puts an enterprise at great risk because security of agency resources is as much a human issue as it is a technology issue ^[17].”

Advanced Threat Detection Systems

Leverage MDR and SIEM systems to detect better threats across an organization's IT environment and security-relevant systems. MDR systems allow data aggregation, analysis, and correlation of data between security data collection sources such as Cloud Applications, Network Devices, and Endpoint Detection and Response sources. Medusa's initial access activity through spear phishing emails to gain endpoint access that exfiltrates data over the network is evidence that protecting against this type of attack requires a multi-source approach.

Conclusion

The Medusa Group's evolving tactics and sophisticated approaches to cyberattacks pose a significant challenge to cybersecurity defenses. A multi-faceted defense strategy, combining technological solutions and human vigilance, is imperative to mitigate the risks associated with this group. Continuous monitoring, rapid response capabilities, and regular updates to security protocols are essential in staying ahead of such advanced threat actors.

NOTABLE CVEs THIS QUARTER

Adlumin noted the following Common Vulnerabilities and Exposures (CVEs), which had especially severe, novel, or widespread impacts.

Vulnerabilities CVE-2023-3519: Analysis and Mitigation Strategies in Citrix Products

CVE-2023-3519 represents a critical vulnerability in certain Citrix products, posing significant risks to enterprise networks and data security.

Vulnerability Details: CVE-2023-3519 is categorized as an unauthenticated, remote code execution vulnerability. It exists in Citrix Netscaler, CitrixApplication Delivery Controller (ADC), and CitrixGateway products, primarily affecting versions 12.1 and later. The vulnerability arises due to Improper Control of Generation of Code ('Code Injection') CWE-94^[18]; this flaw allows attackers to execute arbitrary code remotely, gain system privileges, and access sensitive data.

Attack Vector: Exploitation of CVE-2023-3519 typically involves an unauthenticated, remote attacker issuing HTTP GET Requests handled by the NetScaler Packet Processing Engine (MPSSE), which leads to a buffer overflow^[19]. The complexity of the exploit is low, allowing adoption by multiple threat actors that can leverage publicly available proof of concept exploits for the vulnerability.

Known Usage by Attackers

Attack Patterns: Before its discovery, CVE-2023-3519 had been used in zero-day attacks by threat actors to implant webshells on compromised non-production NetScaler ADC servers, enabling remote access^[20].

Threat Actors: Initial discovery and usage of the exploit appear to be potentially tied to actor(s) within the group FIN8, which deployed BlackCat/ALPHV ransomware in July^[21].

Documented Incidents

Recent research showed that 1,828 NetScaler servers

remain backdoored, of which roughly 1,248 are already patched against the flaw – meaning that access remained beyond patching of the underlying operating system and software^[22]. CISA's initial report documented an incident where threat actors uploaded a compressed TZ file containing a webshell, discovery script, and setuid binary before the actor proceeded with SMB scanning on the subnet. The webshell enabling remote access was used for Active Directory enumeration and data exfiltration, which Adlumin finds consistent with the observed SMB scanning.

Mitigation Strategies

Patching: The primary mitigation step is applying the patches Citrix released to ensure that all affected systems are updated to the latest version that addresses CVE-2023-3519. It's important to note that patching may not remove already installed backdoors and that access may be persistent across reboots.

Network Segmentation: Enhance network security by segmenting networks. This limits the spread of potential exploitation and isolates critical systems from vulnerable ones.

Monitoring and Detection: Implement advanced monitoring tools to detect anomalous activities indicative of CVE-2023-3519 exploitation. Regularly update intrusion detection systems (IDS) and intrusion prevention systems (IPS) with the latest signatures related to this vulnerability.

Access Controls: Strengthen access controls, particularly for systems running the vulnerable Citrix products, and the ability to interface with non-needed servers and systems.

Incident Response Planning: Update incident response plans to include scenarios involving CVE-2023-3519. Conduct regular drills and ensure that response teams are prepared to address potential breaches swiftly and effectively.

Vendor Collaboration: Maintain communication with Citrix for updates and advisories related to CVE-2023-3519. Participate in industry forums and organizations such as the Information Systems Audit and Control Association (ISACA) ^[23], the Information Systems Security Association (ISSA) ^[24], and industry-specific Intelligence Sharing and Analysis Centers (ISACs) ^[25] to stay informed about emerging threats and best practices. Subscribe for vendor-specific security updates for products used in your organization, and as always, watch CISA's Known Exploited Vulnerability (KEV) Catalog to understand the latest vulnerabilities being seen used in the wild^[26].

Conclusion

CVE-2023-3519 poses a severe threat to organizations using affected Citrix products. It is essential to understand the vulnerability's technical aspects, remain vigilant about potential exploitations, and implement robust mitigation strategies to safeguard against this significant cybersecurity risk.



CVE-2023-2868: Critical Vulnerability in Barracuda Email Security Gateway Products

CVE-2023-2868 is a critical remote command injection vulnerability found in Barracuda Email Security Gateway (ESG) appliances, affecting versions 5.1.3.001 to 9.2.0.006. This vulnerability has been actively exploited by threat actors, leading to notable compromises such as the attack on the Australian Capital Territory government^[4].

Technical Details:

Nature of Vulnerability: The vulnerability stems from inadequate sanitization of .tar file processing within the ESG appliances. Specifically, it arises from a failure to comprehensively sanitize user-supplied .tar files, particularly concerning the names of the files within the archive.

Mechanism of Exploit: Attackers can exploit this flaw by formatting file names within a .tar archive in a specific manner. When the vulnerable ESG processes these manipulated .tar files, the specially crafted file names trigger the execution of arbitrary system commands remotely. This is achieved by utilizing Perl's qx operator within the context of the ESG.

Privilege Execution: The executed commands run with the privileges of the ESG product, significantly increasing the impact of the exploit.

Potential Impacts: Once exploited, this vulnerability can lead to several adverse outcomes, such as unauthorized access to sensitive data, data exfiltration, tampering with critical system settings, and even the complete and permanent compromise of the affected system.

Mitigations:

Patching: Barracuda provided a patch (BNSF-36456) to address the vulnerability, which was automatically applied to all customer appliances.

Hardware Replacement Recommendation: Due to the unfixable nature of some hardware appliances, Barracuda has recommended replacing these appliances entirely to mitigate the risk.

Usage by Attackers & Notable Compromises:

This vulnerability has been actively exploited in the wild since at least October 2022. Exploiting this vulnerability by attackers opens affected organizations to significant risks, including financial and reputational damage.

The case of CVE-2023-2868 highlights the critical need for rigorous security practices, including regular vulnerability assessments, prompt patch management, and a readiness to take decisive action, like hardware replacement, when necessary to mitigate risks.



CVE-2023-20198 and CVE-2023-20273: Dual Critical Vulnerabilities in Cisco IOS XE Products

CVE-2023-20198: This vulnerability allows an attacker to gain initial access by issuing a privilege 15 command to create a local user and password combination, thus obtaining normal user access ^[27].

CVE-2023-20273: After gaining initial access, an attacker can exploit CVE-2023-20273 to elevate their privilege to root, enabling them to write an implant to the file system. This vulnerability arises due to insufficient input validation, allowing an attacker to send crafted input to the web UI and subsequently inject commands with root privileges into the underlying operating system ^[28].

Affected Systems

These vulnerabilities specifically affect Cisco IOS XE Software with the web UI feature enabled. This feature is typically enabled through IP HTTP server or IP HTTP secure-server commands. It's an embedded GUI-based system-management tool that comes with the default image and requires no separate enablement or license. It facilitates system provisioning, deployment, management, configuration, and troubleshooting without CLI expertise.

Detection and Compromise Indicators

To identify potential compromises:

1. Check system logs for specific log messages indicating unauthorized user access or unknown local user creation.
2. Look for unfamiliar filenames in system logs, which could indicate file installation actions by an attacker.
3. Use a specific curl command provided by Cisco Talos to check for the presence of the implant on a system ^[28].
 - `curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "https://systemip/webui/logoutconfirm.html?logon_hash=1"`
4. The implant is present if the request returns a hexadecimal string such as 0123456789abcdef01.

Specific IDS rules can also alert to activities associated with these vulnerabilities, such as initial implant injection and implant interaction.

Mitigations

There are no direct workarounds for these vulnerabilities. However, several mitigation strategies can be employed:

Disabling the HTTP Server Feature: Administrators can eliminate the attack vector by disabling the HTTP server feature using no IP HTTP server or no IP HTTP secure-server commands in global configuration mode. If both the HTTP server and the http-secure server are in use, then both commands are required to disable the feature.

Limiting Access to Trusted Networks: Restricting HTTP server access to trusted networks can significantly limit exposure to these vulnerabilities.

It's important to note that while these mitigations have been successful in test environments, their effectiveness can vary based on individual network environments and conditions. As such, each organization should assess the applicability and impact of these mitigations in their specific context.

This vulnerability has been fixed through Cisco patching of the affected devices and software. Organizations with

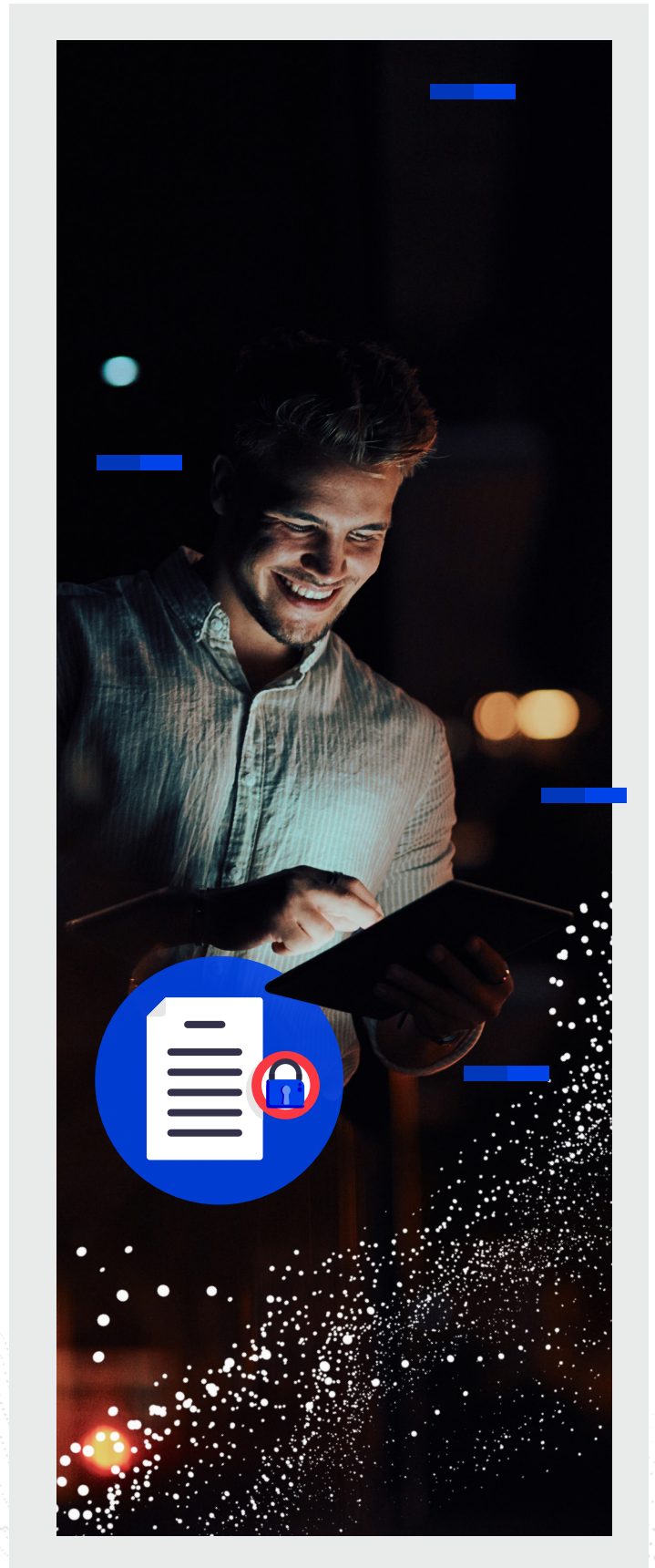
service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

Known Exploitation and Reporting

CVE-2023-20273 is listed in CISA's Known Exploited Vulnerabilities Catalog ^[29]. Organizations are required to verify compliance with specific guidelines and report any positive findings of compromise immediately to CISA.

Conclusion

The exploitation of CVE-2023-20198 and CVE-2023-20273 poses significant risks, allowing attackers to gain unauthorized access and escalate privileges to the root level within affected Cisco IOS XE Software systems. Organizations using these systems should take immediate steps to assess their vulnerability and apply recommended mitigations to protect their networks from potential exploits. Regular monitoring and log analysis are crucial for the early detection of any malicious activities related to these vulnerabilities^[30].



REPORT RECOMMENDATIONS

- ✓ Adlumin has observed continued threats to all industries through double extortion ransomware, usage of publicly available and open-source exploits and toolkits, and the continued development of eCrime groups targeting Zero Day vulnerabilities. To help defend organizations against these modern threats, we recommend Adopting Threat Intelligence and Monitoring; given the constantly evolving nature of threat actors in both the Advanced Persistent Threat (APT) and e-crime space as we see with BianLian and Medusa Ransomware, we recommend organizations should invest in advanced threat intelligence tools and monitoring systems such as EDR / XDR products. These should be capable of detecting unusual network activities, identifying potential breaches, and providing real-time alerts.
- ✓ Having a strong Patch Management process and capability Vulnerabilities such as CVE-2022-3519, CVE-2023-2868, and CVE-2023-20198) highlight the importance of a robust patch management system and process. Regular and timely patching through updates and security patches. This ensures that commonly used and exploited software is kept up-to-date and secure from exploitation by known vulnerabilities. A good patching process can also reduce the time between zero-day discovery and protection. It's essential for critical IT infrastructure such as Citrix products and Cisco networking devices.
- ✓ Adopting Zero Trust Architecture developing and implementing a Zero Trust security architecture and model for your organization can dramatically reduce the risk of unauthorized access and lateral movement within networks. This involves verifying every user and device, regardless of location
- ✓ Network segmentation and access control segmenting networks and implementing strict access controls can limit the impact of a reach by restricting threat actors' movement across the network and access to potentially sensitive data. Networks and services should be restricted based on the principle of least privilege, baselined, and regularly audited.
- ✓ Integrating relevant security data with increasing complexity in networks, applications, architectures, devices used, and even security-relevant systems - it's important to have a platform where data from security-relevant systems such as EDR products can be joined with endpoint logging, network logging, and other integrations. The usage of third-party products and integrations such as cloud services increase the need for centralization of security data through MDR products like Adlumin so that the entire security landscape can be viewed.

ADLUMIN IN THE NEWS

Adlumin uncovered evidence that Play ransomware (also known as PlayCrypt) is now being sold "as a service." Play ransomware has been responsible for attacks on companies and government organizations worldwide since it was first discovered in 2022. Making it available to affiliates that might include sophisticated hackers, less-sophisticated "script kiddies," and various levels of expertise in between could dramatically increase the volume of attacks using the highly successful, Russia-linked Play ransomware.

Read more:

[The Hacker News](#)[Tech Radar](#)


REFERENCES

1. <https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023#1>
2. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a>
3. <https://www.linkedin.com/pulse/medusa-ransomware-attack-cyprus-case-study-evading-abou-chabk%C3%A9>
4. <https://socradar.io/dark-web-profile-medusa-ransomware-medusalocker/>
5. <https://research.nccgroup.com/2023/11/13/dont-throw-a-hissy-fit-defend-against-medusa/>
6. <https://www.picussecurity.com/resource/medusalocker-ransomware-analysis-simulation-and-mitigation>
7. [https://www.cyborgsecurity.com/threats/emerging-threats/medusa/#:~:text=MEDUSA%E2%80%9D\).,The%20ransomware%20claims%20to%20exfiltrate%20data%20from%20compromised%20organizations%20to,a%20ransom%20is%20not%20met.](https://www.cyborgsecurity.com/threats/emerging-threats/medusa/#:~:text=MEDUSA%E2%80%9D).,The%20ransomware%20claims%20to%20exfiltrate%20data%20from%20compromised%20organizations%20to,a%20ransom%20is%20not%20met.)
8. <https://www.nbcnews.com/tech/security/students-psychological-reports-abuse-allegations-leaked-ransomware-hac-rcna79414>
9. <https://www.moneris.com/en/about-moneris/news/false-reports-of-ransomware-impacting-moneris?cmfc=reactive&dsc=owned&trgtaud=general%2Bpublic&cstprs=all&cmpobj=awareness&cntapp=original&cntpll=thought%2Bleadership>
10. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf>
11. <https://www.hhs.gov/sites/default/files/medusalocker-ransomware-analyst-note.pdf>
12. <https://www.microsoft.com/insidetrack/blog/office-365-helps-secure-microsoft-from-modern-phishing-campaigns/>
13. <https://www.searchenginejournal.com/google-spam-fighting-ai/405682/>
14. <https://thecyberexpress.com/medusa-cyber-attacks-karamchand-thapar-windak/>
15. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf>
16. https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf
17. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf>
18. <https://nvd.nist.gov/vuln/detail/CVE-2023-3519>
19. <https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467>
20. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a>
21. <https://www.bleepingcomputer.com/news/security/attacks-on-citrix-netscaler-systems-linked-to-ransomware-actor/>
22. <https://thehackernews.com/2023/08/nearly-2000-citrix-netscaler-instances.html>
23. <https://www.isaca.org/>
24. <https://www.issa.org>
25. <https://www.nationalisacs.org>
26. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
27. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/%20cisco-sa-iosxe-webui-privesc-j22SaA4z>
28. <https://nvd.nist.gov/vuln/detail/CVE-2023-20273>
29. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1>
30. <https://www.csoonline.com/article/575545/act-government-falls-victim-to-barracuda-s-esg-vulnerability.>



ILLUMINATE THREATS AND ELIMINATE RISKS

Learn more about how Adlumin's Managed Detection and Response Services and Security Operations Platform can empower your team to illuminate threats, eliminate cyber risk, and command authority; contact us today or schedule a demo at www.adlumin.com.



About Adlumin

Adlumin Inc. provides the enterprise-grade security operations platform and managed detection and response (MDR) services that keep mid-market organizations secure. With one license and one platform, its patented technology gives organizations and solution providers everything they need for effective threat hunting, incident response, vulnerability management, darknet exposure monitoring, compliance support and much more.

The Adlumin platform is feature-rich enough for organizations to operate on their own, yet built specifically to amplify the skills and capabilities of managed service providers who use it to deliver cutting-edge security that can scale to meet the needs of any operating environment. With full access to the platform regardless of whether they are running it themselves or relying on Adlumin's MDR services or expert partners, Adlumin gives organizations unparalleled visibility into their security posture through access to alerts, investigation data, threat intelligence, compliance reporting and everything else – all in real time.

