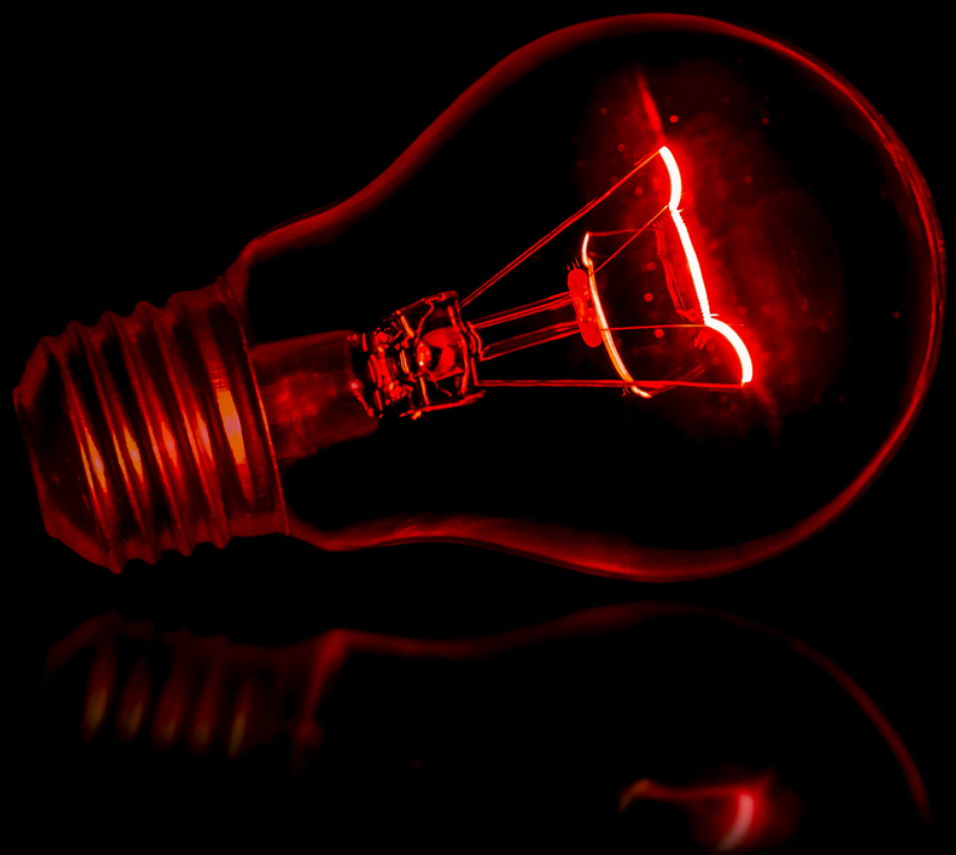
Threat Intel Roundup: Confluence, Outlook, Trello, Agniane



Week in Overview(16 Jan-23 Jan] - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. Agniane Stealer
Overview:
Agniane Stealer is an advanced information stealer discovered by cybersecurity researchers. It operates as part of the Malware-as-a-Service (MaaS) platform, specifically linked to the Cinoshi Project. The stealer is adept at extracting sensitive data, including credentials, system information, and crypto-related details.
Key Features:

- **Credential Theft:** Agniane Stealer targets web browsers, Telegram, Discord, Steam, WinSCP, and Filezilla sessions.
- **Cryptocurrency Focus:** Supports over 70 crypto extensions and 10+ crypto wallets.
- **Evasion Techniques:** Implements anti-analysis measures to detect and evade security tools.
- **Dark Web Availability:** Actively promoted and sold on a dedicated Telegram channel, possibly managed by the malware author.

2. Trello Allegedly Breached
Incident Overview:
A cybercriminal known as 'emo' claims to have breached Trello, offering a database of 15,115,516 user records for sale. The compromised data includes emails, usernames, full names, and other account information.
Implications:

- Potential exposure of user credentials and personal information.
- Increased risk of account takeover and phishing attacks.

3. Cyber Kill Chain® and TeamCity Vulnerability Exploitation
Incident Summary:
Researchers identified a critical vulnerability (CVE-2023-42793) in TeamCity, a build management server. The exploit allows remote code execution, leading to active exploitation by threat actors. The FortiGuard Incident Response team conducted an investigation into a compromised US-based biomedical manufacturing organization.
Attack Highlights:

- **Vulnerability Exploitation:** Successful exploitation of CVE-2023-42793 using a Python exploit script.
- **Multiple Threat Actors:** Evidence suggests simultaneous operations by various threat actors.
- **Command Execution:** Threat actors executed diverse commands on the compromised server, indicating broad malicious activity.

4. The Confusing History of F5 BIG-IP RCE Vulnerabilities
Incident Background:
F5 BIG-IP, a popular networking device, faced a series of Remote Code Execution (RCE) vulnerabilities, leading to confusion in the cybersecurity community. The incidents involved multiple vulnerabilities, each with its own set of challenges and mitigations.
Key Points:

- **Multiple Vulnerabilities:** The F5 BIG-IP platform experienced a succession of RCE vulnerabilities.
- **Community Response:** Cybersecurity professionals navigated through the challenges of understanding, addressing, and mitigating the diverse set of vulnerabilities.
- **Importance of Patching:** The incidents underscored the critical role of timely patching in mitigating evolving threats.

5. Exploitation of Apache ActiveMQ Flaw (CVE-2023-46604)
Incident Overview:
A critical vulnerability (CVE-2023-46604) in Apache ActiveMQ was exploited to deliver the Godzilla web shell. The flaw allowed unauthorized remote code execution, enabling threat actors to compromise systems.
Attack Details:

- **Vulnerability Exploitation:** Exploited CVE-2023-46604 to execute the Godzilla web shell.
- **Unauthorized Code Execution:** Threat actors gained remote access, posing a significant security risk.
- **Security Recommendations:** Emphasizes the importance of promptly patching and securing messaging systems.

6. Outlook Exploit Leads to NTLM v2 Password Breach (CVE-2023-35636)
Incident Summary:
An Outlook exploit (CVE-2023-35636) resulted in a breach where NTLM v2 passwords were compromised. The vulnerability allowed threat actors to execute arbitrary code and extract sensitive information.
Attack Highlights:

- **Outlook Vulnerability:** Exploited CVE-2023-35636 for arbitrary code execution.
- **Password Breach:** NTLM v2 passwords compromised, posing a risk to user accounts.
- **Mitigation Strategies:** Urges organizations and users to apply patches and maintain vigilant security practices.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- Agniane Stealer
- Trello Allegedly Breached
- Cyber Kill Chain® and TeamCity Vulnerability Exploitation
- The Confusing History of F5 BIG-IP RCE Vulnerabilities
- Exploitation of Apache ActiveMQ Flaw to Deliver Godzilla Web Shell (CVE-2023-46604)
- Outlook Exploit Leads to NTLM v2 Password Breach (CVE-2023-35636)
- Atlassian Confluence Remote Code Execution (CVE-2023-22527)

🚨 Vulnerability of the Week

Confluence CVE-2023-22527

A critical vulnerability has been identified in Atlassian's Confluence Server and Data Center, marked as CVE-2023-22527. This vulnerability allows unauthenticated attackers to inject OGNL expressions into a Confluence instance, leading to the execution of arbitrary code and system commands. The vulnerability affects older versions of Confluence Server and Data Center, and immediate action is required for affected instances.

Initial Analysis

Upon analyzing the CVE description provided by Atlassian, it was observed that version 8.5.5 completely eliminates the vulnerability. However, the vulnerability was initially rendered unexploitable in version 8.5.4. The analysis involved comparing changes between versions 8.5.3 and 8.5.4, focusing on files with OGNL-related modifications.

Identifying the Unauthenticated Attack Surface

Discovering that Confluence views could be accessed directly by hitting *.vm files, the research team looked for template files accepting parameters passed to potentially dangerous sinks. Notable files such as **confluence/template/xhtml/pagelist.vm** and **confluence/template/aui/text-inline.vm** were identified as potential attack vectors.

OGNL Expression Evaluation

After modifying the payload to bypass security restrictions, the research team successfully executed OGNL expressions, leading to code execution. A failed attempt triggered a security measure blocking expressions longer than ~200 characters, but a small payload adjustment utilizing the #parameters map allowed successful execution of system commands.

Exploitation Mitigation

Atlassian has addressed this vulnerability in the most recent versions of Confluence Server and Data Center. Users are strongly advised to update their instances to version 8.5.5 or the latest supported version. The research team has also contributed a Nuclei template (https://github.com/projectdiscovery/nuclei-templates/pull/8982) to assist in detecting instances vulnerable to CVE-2023-22527.

Impact

This vulnerability, if exploited, allows unauthenticated attackers to achieve remote code execution on affected Confluence instances. The severity is classified as critical, with a CVSS score of 10.

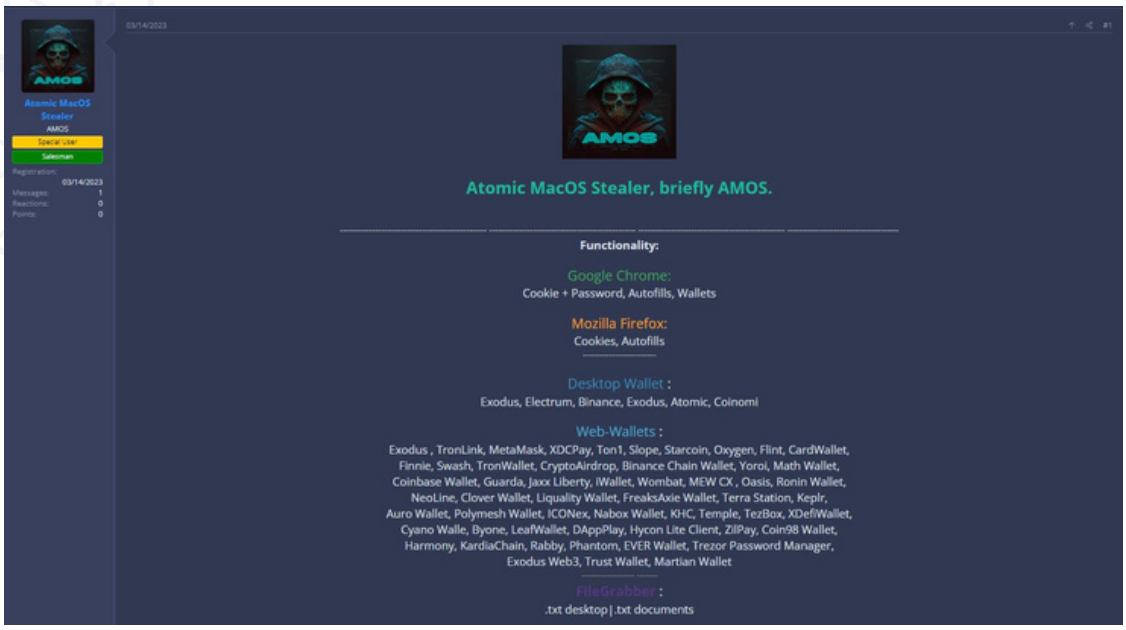
Recommendations

- **Immediate Update:** Upgrade Confluence instances to version 8.5.5 or the latest supported version.
- **Detection:** Utilize the provided Nuclei template for detecting instances vulnerable to CVE-2023-22527.
- **Monitoring:** Monitor network traffic for potential exploitation attempts.

References

- Atlassian Security Advisory
- Atlassian Jira Issue
- ProjectDiscovery Blog Post

😰 Malware or Ransomware



https://twitter.com/AnFam17/status/1749641174099394655

RussianPanda, a cybersecurity researcher, recently shed light on Agniane Stealer, categorizing it as a copycat project emerging from the developer of #AgnianeStealer. The report highlights Agniane Stealer's fraudulent activities, including credential theft, system information extraction, and session details hijacking from various applications. This stealer is specifically notable for its focus on cryptocurrency-related data, targeting extensions and wallets for illicit gains.

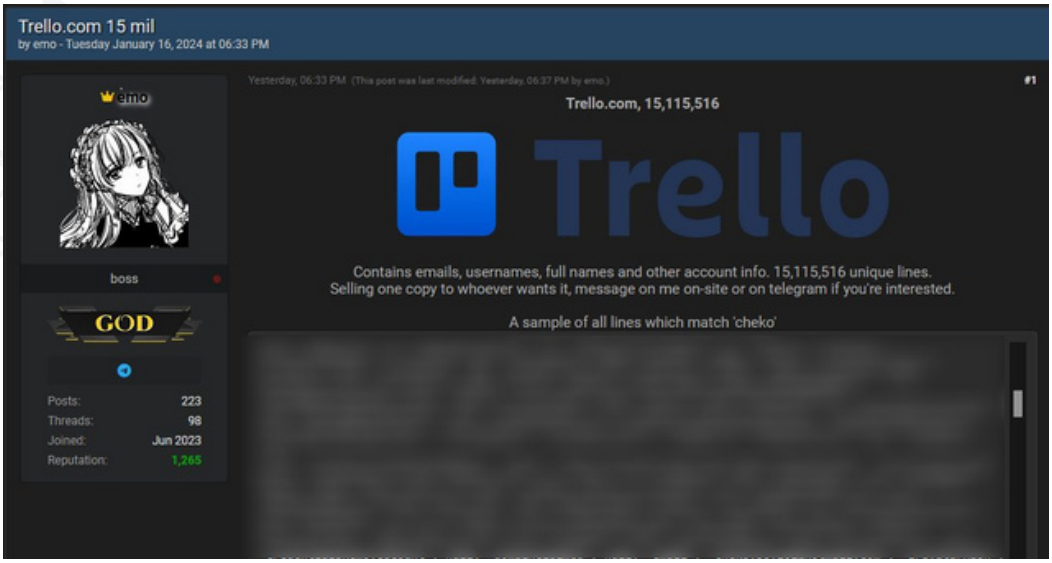
1. Malware-as-a-Service (MaaS) Platform Connection
RussianPanda suggests that Agniane Stealer is likely affiliated with the Cinoshi Project, a Malware-as-a-Service platform discovered in early 2023. The close association indicates that Agniane Stealer is available for sale on dark web forums, sharing infrastructure and code elements with the MaaS platform.
2. Stealing Capabilities
Agniane Stealer is an information stealer with diverse capabilities:
- **Credential Theft:** Gathers stored credentials from web browsers, Telegram, Discord, Steam, WinSCP, and Filezilla sessions.
- **Cryptocurrency Focus:** Displays extensive support for over 70 crypto extensions and 10+ crypto wallets.
- **System Information Extraction:** Captures screenshots, OpenVPN profiles, and comprehensive details about the victim's computer.

3. Evasion Techniques
Agniane Stealer employs various evasion methods to counter anti-analysis measures:
- **Anti-Analysis Detection:** Can identify malware sandboxes, emulators, VirtualBox, and other analysis tools.
- **Build Protection:** Features configurations to prevent execution on virtual machines, emulators, and block scanning on services like Virustotal and AnyRun.

4. Availability and Promotion
The report uncovers a Telegram channel actively promoting and selling Agniane Stealer. The channel, possibly managed by the malware author, consistently posts updates, feature lists, and pricing details.
5. Pricing Information
The pricing details revealed in the report indicate subscription-based access to Agniane Stealer:
- **Monthly Subscription:** $50
- **Three-Month Subscription:** Initially $150, discounted to $120 (20% off)
- **Lifetime Subscriptions:** Not available for sale.

Implications and Recommendations
Given the evolving threat landscape associated with Agniane Stealer, the report suggests heightened vigilance and cybersecurity measures. It emphasizes the need for organizations and users to implement robust security practices, including regular system updates, anti-malware solutions, and user education to thwart potential threats associated with information stealers like Agniane Stealer.

Leakage



https://twitter.com/H4ckManac/status/1747527579559411959

In a recent cybersecurity development, the popular project management platform Trello has allegedly fallen victim to a data breach. The cybercriminal, self-identified as 'emo,' purports to have compromised Trello's security, obtaining a database containing 15,115,516 user records. The compromised data reportedly encompasses sensitive information, including emails, usernames, full names, and additional account details.

Breach Details

- **Perpetrator:** The individual behind the breach identifies themselves as 'emo,' suggesting a potential threat actor or hacker responsible for the unauthorized access to Trello's user database.
- **Compromised Database:** The breached database is reported to contain 15,115,516 user records. The nature of the compromise implies that a significant amount of user information is now in the hands of cybercriminals.
- **Stolen Information:** The stolen data comprises critical user details, including emails, usernames, full names, and various other account-related information. This extensive dataset could potentially lead to various cyber threats, including phishing attacks, identity theft, and unauthorized account access.

Potential Implications

- **Phishing Attacks:** The exposure of user emails and additional account information poses a significant risk of phishing attacks. Cybercriminals may leverage this data to craft convincing phishing campaigns, attempting to trick users into disclosing sensitive information or login credentials.
- **Identity Theft:** With full names and usernames in the compromised dataset, users are susceptible to identity theft. Cybercriminals could exploit this information for fraudulent activities, opening avenues for financial fraud or other malicious actions.
- **Account Takeovers:** The stolen data, including usernames and potentially passwords, could be utilized for unauthorized access to Trello accounts. Account takeovers may lead to unauthorized control over projects, exposure of confidential information, or other malicious activities within the platform.

THREATRADAR
By HADESS

TTP Analysis

In September 2023, researchers from Sonar identified a critical vulnerability (CVE-2023-42793) in TeamCity On-Premises, a build management and continuous integration server developed by JetBrains. This vulnerability, with a high CVE score of 9.8, allows for remote code execution without authentication. Rapid7 released a public exploit for this vulnerability on September 27, 2023. The exploit gained notoriety as it was actively exploited in the wild, prompting its inclusion in CISA's 'Known Exploited Vulnerabilities Catalog' on October 4, 2023.

In mid-October 2023, FortiGuard Incident Response (IR) discovered an intrusion into a US-based biomedical manufacturing organization, resulting from the TeamCity vulnerability. This article details the investigation conducted by the FortiGuard IR team, encompassing containment, eradication, and remediation efforts.

Summary of Attack
The victim organization fell prey to the CVE-2023-42793 exploit, leading to a compromise by threat actors, later identified as APT29. highlights key events from the initial discovery of the vulnerability to the containment and remediation efforts.

Vulnerability Exploitation
The FortiGuard IR team initiated the investigation by examining EDR events on the victim's Windows application server (HOST_1_TEAMCITY). Despite the victim having recently updated TeamCity to a non-vulnerable version, evidence of successful exploitation surfaced in the application logs.
The teamcity-auth.log file revealed authentication bypass attempts. Further analysis of the teamcity-server.log file exposed remote code execution evidence, providing insight into the commands executed through exploitation.

Commands executed by multiple threat actors were diverse, indicating simultaneous operations. Notably, some threat actors attempted Linux commands on a Windows server, suggesting varied levels of success.

Remote IP AddressCommands Executed
167.179.75.213
Command line: whoami
154.26.133.111
Command line: bash -c "nproc 2>&1"
104.207.152.236
Command line: cmd.exe "/c whoami"

Nuclei Scanning
Several commands aligned with the use of the Nuclei vulnerability scanner, identified by a corresponding yaml template (CVE-2023-42793.yaml). This template produced echo commands on exploited TeamCity servers, mirroring observed commands in the logs. Correlating logs showcased multiple echo commands indicative of Nuclei scanning .

Main Threat Actor Intrusion
The main threat actor, distinguishable from others, employed Nuclei for identification before executing discovery commands. Following successful exploitation, the actor attempted to download a DLL file, 'AclNumsInvertHost.dll,' and create a scheduled task for persistence. The scheduled task, named "\Microsoft\Windows\DefenderUPDService," referenced the downloaded DLL file.
The main threat actor displayed a sophisticated modus operandi, utilizing the TeamCity vulnerability for initial access, conducting reconnaissance, and establishing persistence.

https://twitter.com/blackorbird/status/1749656832166318099

1Day

https://twitter.com/__kokumoto/status/1749453342420643947

Security researchers from Trustwave have observed a significant increase in attacks exploiting a now-patched vulnerability (CVE-2023-46604) in Apache ActiveMQ. Threat actors leverage this flaw to deliver the Godzilla web shell, allowing them to gain unauthorized access and control over targeted systems. The attackers hide the web shell within an unknown binary format to evade security and signature-based scanners successfully.

Technical Details

CVE-2023-46604 and Apache ActiveMQ

CVE-2023-46604 is a critical remote code execution vulnerability affecting Apache ActiveMQ, an open-source message broker software used for message-oriented middleware (MOM) purposes. The flaw allows remote attackers to execute arbitrary shell commands by manipulating serialized class types in the OpenWire protocol.

Apache ActiveMQ versions affected by this vulnerability include:

- ActiveMQ 5.18.0 before 5.18.3
- ActiveMQ 5.17.0 before 5.17.6
- ActiveMQ 5.16.0 before 5.16.7
- ActiveMQ before 5.15.16
- ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3
- ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6
- ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7
- ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16

The flaw was addressed by Apache with the release of new ActiveMQ versions on October 25, 2023.

Exploitation Techniques

In observed attacks, the malicious file was planted in the "admin" folder within the ActiveMQ installation directory. This folder contains server scripts for the ActiveMQ administrative and web management console. Notably, the Jetty JSP engine, integrated into ActiveMQ, parsed, compiled, and executed the embedded Java code encapsulated in the unknown binary.

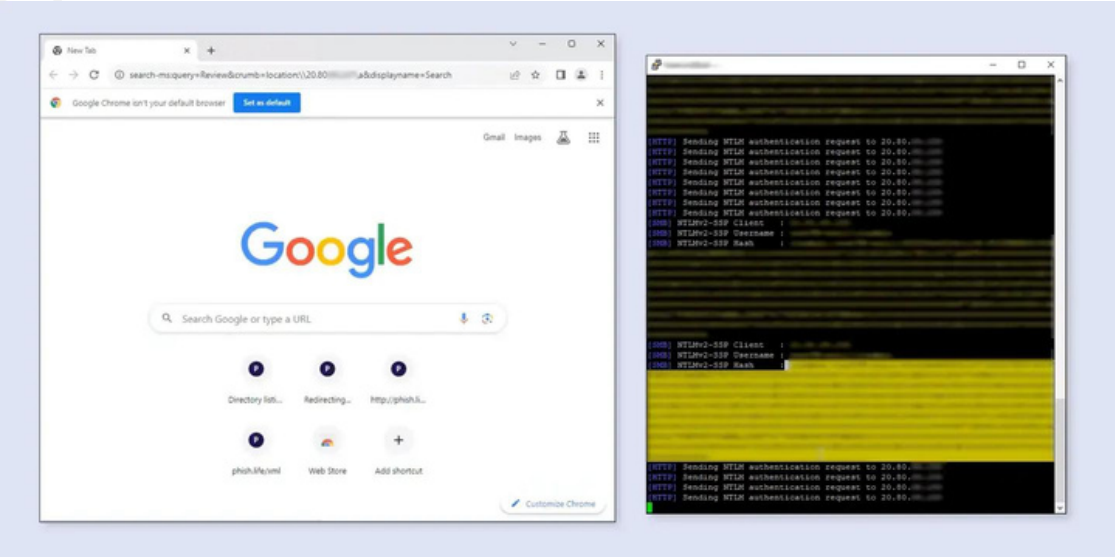
Once deployed, the Godzilla web shell provides threat actors with complete control over the compromised system, allowing for various malicious activities, including viewing network details, conducting port scans, executing Mimikatz commands, running Meterpreter commands, executing shell commands, remotely managing SQL databases, and handling file management tasks.

Mitigation Steps

To mitigate the risks associated with CVE-2023-46604 and potential Godzilla web shell attacks:

- **Update ActiveMQ:** Ensure that Apache ActiveMQ is updated to the latest patched versions (5.18.3, 5.17.6, 5.16.7, or later).
- **Regular Security Audits:** Conduct regular security audits to identify and address potential vulnerabilities in your systems.
- **Monitor Admin Folder:** Regularly monitor the "admin" folder within the ActiveMQ installation directory for any suspicious files or activities.
- **Network Monitoring:** Implement network monitoring to detect anomalous traffic patterns and potential exploitation attempts.

🌶️ Trending Exploit



https://twitter.com/Dinosn/status/1748197821021331656

A significant security vulnerability has been identified in Microsoft Outlook, marked as CVE-2023-35636, which exposes NTLM v2 hashed passwords during the calendar sharing function. This vulnerability allows attackers to intercept sensitive information, potentially leading to unauthorized access to systems and user data.

CVE-2023-35636 and NTLM v2

CVE-2023-35636 is a critical security vulnerability found in Microsoft Outlook, specifically within the calendar sharing functionality. Exploiting this vulnerability allows attackers to intercept NTLM v2 hashed passwords, which are crucial for authentication in Microsoft Windows systems. Despite NTLM v2 being more secure than its predecessor, it remains susceptible to offline brute-force and authentication relay attacks.

Exploitation Scenarios

Attackers can leverage the obtained NTLM v2 hashes in two primary scenarios:

1. **Offline Brute-Force Attack:** Attackers attempt to crack user passwords by trying various combinations against the NTLM v2 hash. This attack is undetectable as it leaves no network traces.
2. **Authentication Relay Attack:** Attackers intercept NTLM v2 authentication requests, relaying them to a different server, potentially gaining unauthorized access to the victim's intended server.

Outlook Exploit

The Outlook exploit involves adding specific headers to an email, directing Outlook to share content and contact a designated machine. By manipulating these headers ("Content-Class" and "x-sharing-config-url"), attackers create an opportunity to intercept NTLM v2 hashes during the authentication process.

Other Attack Vectors

Apart from Outlook, attackers can exploit Windows Performance Analyzer (WPA) and Windows File Explorer to access NTLM v2 hashes. These attacks involve tricking applications into revealing sensitive information through URI handlers and specific parameters.

Mitigation Steps

Microsoft has released a patch on December 12, 2023, addressing the Outlook vulnerability (CVE-2023-35636), categorizing it as "important." However, vulnerabilities associated with WPA and Windows File Explorer are considered of "moderate severity" by Microsoft.

To safeguard systems from NTLM v2 attacks:

1. **SMB Signing:** Enable SMB signing to protect against tampering and man-in-the-middle attacks.
2. **Block Outgoing NTLM v2:** For Windows 11 (build 25951) and above, block outgoing NTLM authentication.
3. **Force Kerberos Authentication:** Enforce Kerberos authentication and block NTLM v2 where not required.

The Topic of the Week

CVE	Description	tag
CVE-2021-22986	Authentication Bypass via SSRF	Tag
CVE-2022-1388	Auth Bypass via Header Smuggling	Tag
CVE-2021-23015	Post-authentication RCE via Command Injection	Tag
CVE-2022-41800	Post-authentication RCE via .rpmspec Injection	Tag
n/a	Post-authentication RCE via `/mgmt/tm/util/bash`	Tag

https://www.labs.greynoise.io/grimoire/2024-01-14-f5-rce-explained/

GreyNoise Labs' Ron Bowes provides a comprehensive overview of F5 BIG-IP Remote Code Execution (RCE) vulnerabilities that have emerged since 2020. The report aims to clarify the distinct vulnerabilities and their implications when encountered in logs.

Vulnerabilities Discussed

1. CVE-2021-22986: Authentication Bypass via SSRF

- **Description:** Involves an authentication bypass exploited through Server-Side Request Forgery (SSRF).
- **Detection Tag:** CVE-2021-22986 Tag
- **Exploitation:** Utilizes the **/mgmt/shared/authn/login** endpoint, potentially leading to post-authenticated RCE.

2. CVE-2022-1388: Auth Bypass via Header Smuggling

- **Description:** Authentication bypass due to header injection.
- **Detection Tag:** CVE-2022-1388 Tag
- **Exploitation:** Exploits localhost-only Jetty server with the **/mgmt/tm/util/bash** endpoint.

3. CVE-2021-23015: Post-authentication RCE via Command Injection

- **Description:** Post-authentication RCE through command injection.
- **Detection Tag:** CVE-2021-23015 Tag
- **Exploitation:** Involves a POST request to **/mgmt/shared/authn/login** with a malicious **filePath** parameter.

4. CVE-2022-41800: Post-authentication RCE via .rpmspec Injection

- **Description:** RCE through .rpmspec injection post-authentication.
- **Detection Tag:** CVE-2022-41800 Tag
- **Exploitation:** Exploits the **/mgmt/shared/iapp/rpm-spec-creator** endpoint with crafted data.

5. Post-authentication RCE via /mgmt/tm/util/bash

- **Description:** Exploiting the **/mgmt/tm/util/bash** endpoint for post-authentication RCE.
- **Detection Tag:** General F5 RCE Tag
- **Exploitation:** Requires authentication, potentially combined with other vulnerabilities for effective exploitation.

Notable Observations and Challenges

- Identification of various features that appear as vulnerabilities but are not technically classified as such.
- Authentication bypass techniques often involve leveraging the **/mgmt/tm/util/bash** endpoint for code execution.
- Instances of confusing scenarios where multiple vulnerabilities seem to overlap, leading to challenges in tracking and understanding.

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Threat Radar
WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.