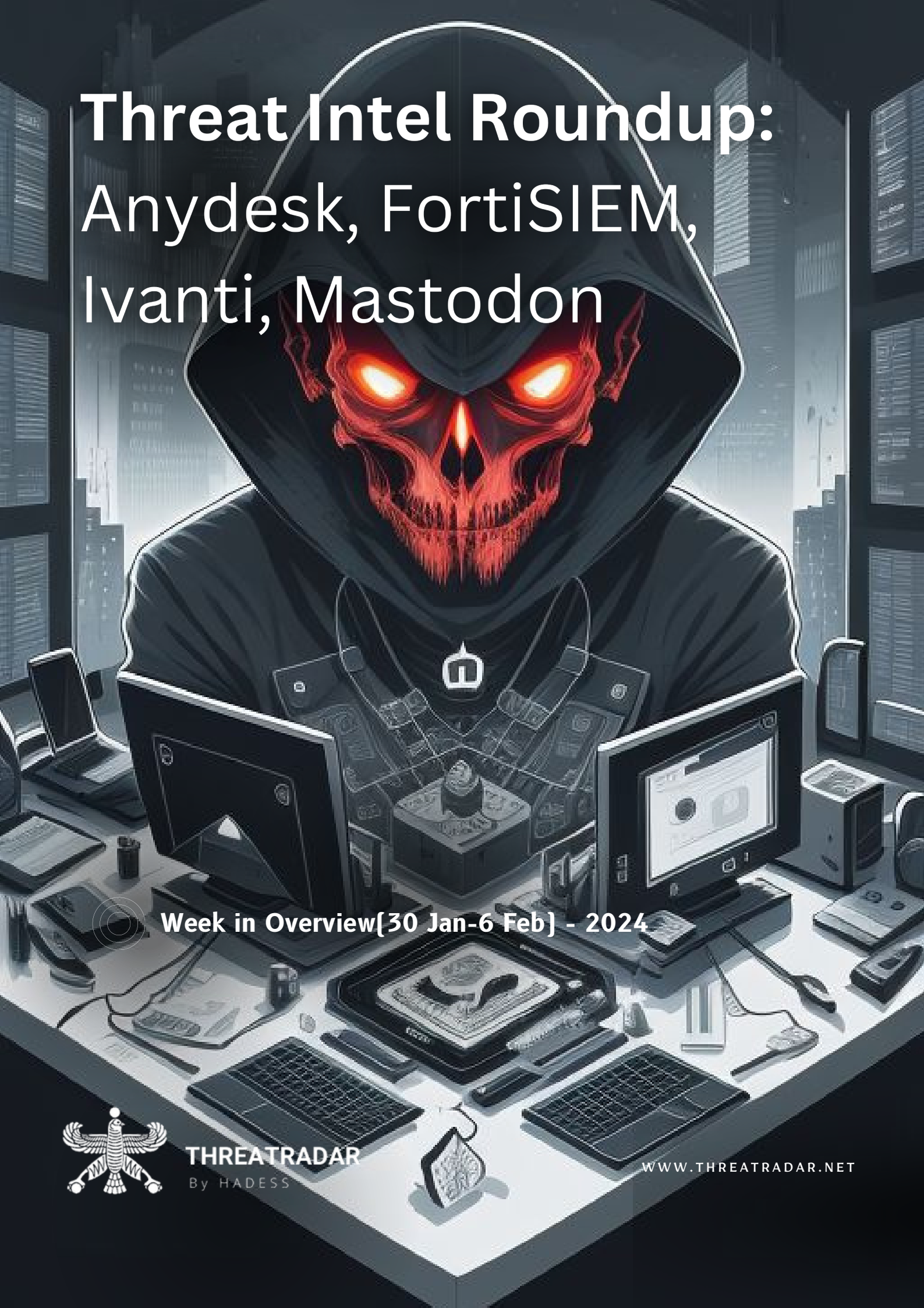
Threat Intel Roundup: Anydesk, FortiSIEM, Ivanti, Mastodon



Week in Overview{30 Jan-6 Feb} - 2024

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **Discovery of VajraSpy RAT in Android Apps**:
   - ESET researchers discovered twelve Android apps containing the VajraSpy Remote Access Trojan (RAT) used by the Patchwork APT group.
   - Six of these apps were previously available on Google Play, accumulating over 1,400 installs.
   - The apps, advertised as chat applications, share the same malicious code and belong to the VajraSpy malware family operated by the Patchwork APT group.
2. **Critical Vulnerability in Mastodon (CVE-2024-23832)**:
   - Mastodon disclosed a critical vulnerability, CVE-2024-23832, stemming from an origin validation error, potentially leading to account takeover.
   - The vulnerability affects Mastodon versions prior to 3.5.17, prompting administrators to update their servers promptly to prevent exploitation.
   - Specific details about the vulnerability are expected to be released on February 15, 2024.
3. **Vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure**:
   - Ivanti disclosed CVE-2024-21893, a server-side request forgery (SSRF) issue affecting Ivanti Connect Secure and Ivanti Policy Secure.
   - The vulnerability, along with previously chained vulnerabilities, poses risks of unauthenticated remote code execution.
4. **Vulnerability in FortiSIEM Software Allows Unauthorized Code Execution**:
   - A vulnerability in FortiSIEM software allows unauthorized code execution, potentially exploited by threat actors for malicious purposes.
5. **Uncovering a Multi-Stage Malware Campaign Orchestrated by Vietnamese-Based Hacking Group**:
   - Details about a multi-stage malware campaign orchestrated by a Vietnamese-based hacking group are revealed, shedding light on their tactics and techniques.
6. **AnyDesk Cyberattack and Response**:
   - Information regarding a cyberattack involving AnyDesk, a remote desktop software, and the subsequent response measures undertaken to mitigate the attack.
7. **ResumeLooters Malicious Campaign Targeting Job Search Platforms**:
   - Insights into a malicious campaign dubbed ResumeLooters, targeting job search platforms, potentially compromising sensitive information of job seekers.

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:

- Discovery of VajraSpy RAT in Android Apps
- Critical Vulnerability in Mastodon (CVE-2024-23832)
- Vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure
- Vulnerability in FortiSIEM Software Allows Unauthorized Code Execution
- Uncovering a Multi-Stage Malware Campaign Orchestrated by Vietnamese-Based Hacking Group
- AnyDesk Cyberattack and Response
- ResumeLooters Malicious Campaign Targeting Job Search Platforms

🚨 Vulnerability of the Week

FortiSIEM CVE-2024-23109

Fortinet FortiSIEM, versions 6.4.0 through 7.1.1, has been found vulnerable to an "improper neutralization of special elements used in an OS command" (OS command injection) flaw. This vulnerability allows attackers to execute unauthorized code or commands through crafted API requests, posing a significant security risk to affected systems.

Key Findings:

1. Vulnerability Description:
   - The vulnerability (CWE-78) stems from improper neutralization of special elements in OS commands, which can be exploited by remote unauthenticated attackers via crafted API requests.
   - Affected versions include FortiSIEM 6.4.0 through 6.4.2, 6.5.0 through 6.5.2, 6.6.0 through 6.6.3, 6.7.0 through 6.7.8, 7.0.0 through 7.0.2, and 7.1.0 through 7.1.1.
2. Impact:
   - Exploiting this vulnerability could lead to the execution of unauthorized commands or code on the targeted system, potentially compromising its security and integrity.
3. Affected Products:
   - FortiSIEM versions 6.4.0 through 6.4.2
   - FortiSIEM versions 6.5.0 through 6.5.2
   - FortiSIEM versions 6.6.0 through 6.6.3
   - FortiSIEM versions 6.7.0 through 6.7.8
   - FortiSIEM versions 7.0.0 through 7.0.2
   - FortiSIEM versions 7.1.0 through 7.1.1
4. Solutions:
   - Fortinet recommends upgrading to the following versions or above to mitigate the vulnerability:
     - FortiSIEM 7.1.2 or above
     - Upcoming FortiSIEM 7.2.0 or above
     - Upcoming FortiSIEM 7.0.3 or above
     - Upcoming FortiSIEM 6.7.9 or above
     - Upcoming FortiSIEM 6.6.5 or above
     - Upcoming FortiSIEM 6.5.3 or above
     - Upcoming FortiSIEM 6.4.4 or above
5. Acknowledgement:
   - Fortinet acknowledges the responsible disclosure of this vulnerability by security researcher Zach Hanley (@hacks_zach) of Horizon3.ai.

😰 Malware or Ransomware

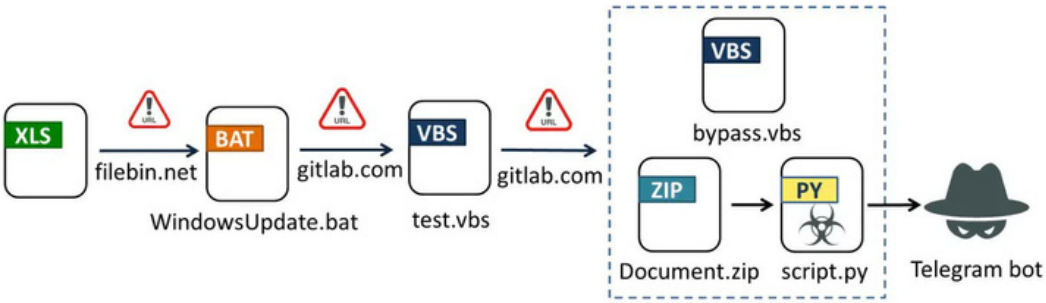
https://twitter.com/GroupIB_TI/status/1754766522982281313

In November 2023, Group-IB's Threat Intelligence unit identified a significant malicious campaign targeting employment agencies and retail companies in the Asia-Pacific (APAC) region. This campaign aimed to steal and sell sensitive user data, particularly from job seekers. The threat actor behind this campaign, identified as ResumeLooters, utilized tactics including SQL injection attacks and Cross-Site Scripting (XSS) to compromise websites and extract personal data and CVs.

Key Findings:

1. ResumeLooters has been active since early 2023, with a focus on conducting SQL injection and XSS attacks against recruitment and retail websites primarily in the Asia-Pacific region.
2. Between November and December 2023, the gang successfully compromised 65 websites, stealing a total of 2,188,444 rows of data, including 510,259 rows of user data from job search websites.
3. The main targets of ResumeLooters are companies in India, Taiwan, Thailand, and Vietnam, although compromised companies were also identified in other regions such as Brazil, the USA, Turkey, Russia, Mexico, and Italy.
4. The group employs various penetration testing tools on their malicious servers, including sqlmap, Acunetix, Beef Framework, X-Ray, Metasploit, ARL (Asset Reconnaissance Lighthouse), and Dirsearch.
5. SQL injection via sqlmap is the group's primary initial vector for compromising websites, with XSS scripts also being injected into legitimate job search websites.
6. Analysis of stolen HTML files revealed the execution of malicious XSS scripts on at least four websites, indicating attempts to obtain admin credentials through phishing forms.
7. The attackers advertised the sale of compromised data in Chinese-speaking hacking-themed Telegram groups.

Art of Detection



https://twitter.com/Dinosn/status/1754736114001228186

In January 2024, FortiGuard Labs identified a sophisticated malware campaign orchestrated by a Vietnamese-based hacking group, previously active in August and September 2023. This campaign, facilitated through a malicious Excel document, presents a significant cybersecurity threat due to its use of multi-stage downloaders and obfuscation techniques.

Key Findings:

1. Initial Attack Vector:
   - The campaign begins with a malicious Excel document containing a VBA script, which triggers the execution of a PowerShell command. This command downloads a seemingly innocuous file, Windows Update.bat, from filebin.net.
2. Multi-Stage Downloaders:
   - Windows Update.bat serves as the initial gateway, hiding its true intentions beneath layers of obfuscation. Abobus obfuscator, non-English characters, and escape characters obscure the malicious code.
   - Upon execution, Windows Update.bat downloads test.vbs, which orchestrates a triple download. It retrieves script.py (the info-stealer), Document.zip (Python 3.11 with required libraries), and bypass.vbs (the Python executor).
3. Malicious Payload:
   - Script.py, reminiscent of a previous campaign in August 2023, is designed to steal browser cookies and login data. It targets a wide range of browsers, including localized ones like the Cốc Cốc browser.
   - The stolen data is compressed and sent to an attacker-controlled Telegram bot.
4. Insight into Hacker Group:
   - The campaign draws from open platforms, offering insights into the hacker group's activities. Repositories and files related to the campaign reveal similarities with other malware such as XWorm, VenomRat, and RedLine.
5. Evolving Tactics:
   - The investigation uncovers emerging tactics, including luring victims into enabling macros in Word documents and concealing dll files within images. Threat actors cleverly use cookies as bait, highlighting their evolving techniques.

THREATRADAR
By HADESS

TTP Analysis

ESET researchers, led by @LukasStefanko

Discovery:
- ESET researchers uncovered twelve Android apps harboring the VajraSpy Remote Access Trojan (RAT) utilized by the Patchwork APT group.
- Six of these apps were previously available on Google Play, accumulating over 1,400 installs before removal.

App Characteristics:
- Except for one news app, the rest were promoted as chat applications.
- Shared malicious code and class names indicate belonging to the VajraSpy malware family.

VajraSpy RAT:
- Customizable RAT employed by the Patchwork APT group.
- Functionality varies based on permission settings, enabling data exfiltration such as contacts, files, SMS messages, call recording, and photo capture.

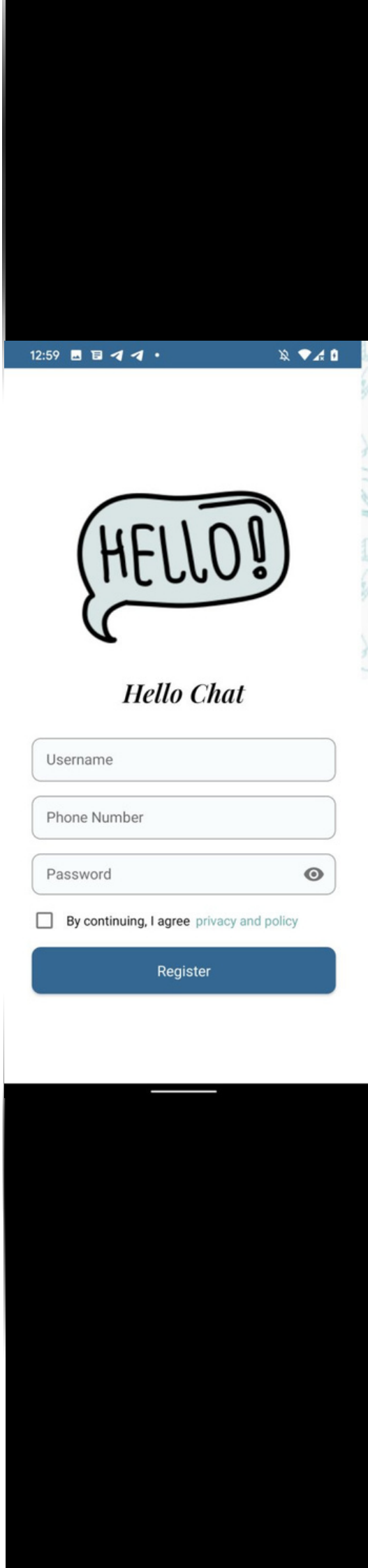
Timeline:
- Apps surfaced online between April 2021 and October 2023.

Targeted Users:
- Predominantly targeted users in Pakistan.
- Tactics included using the name of a prominent Pakistani cricket player as a developer and defaulting to the PK country calling code on login screens.

Indicators of Compromise (IoCs):
- IoCs available on GitHub at https://github.com/eset/malware-ioc/tree/master/vajraspy

Recommendation:
- Android users, particularly in Pakistan, should remain vigilant and verify the authenticity of apps before installation.
- Employ security measures and consider utilizing reputable antivirus software to detect and prevent RAT infections.

https://twitter.com/ESETresearch/status/1753008844454707380



1Day

CVE Identifier: CVE-2024-23832 (CVSS: 9.4)

Vulnerability Description:
- Origin validation error in Mastodon, potentially leading to account takeover.
- Severity rated as critical (CVSS score of 9.4), indicating significant risk.
- Specific details of the vulnerability to be disclosed on February 15, 2024.

Affected Versions:
- All Mastodon versions prior to 3.5.17
- Includes versions 4.0.x before 4.0.13, 4.1.x before 4.1.13, and 4.2.x before 4.2.5

Platform Overview:
- Mastodon is an open-source social network with decentralized servers.
- Admins manage separate servers with individual rules.
- Gained popularity as an alternative to Twitter, particularly within the security community.

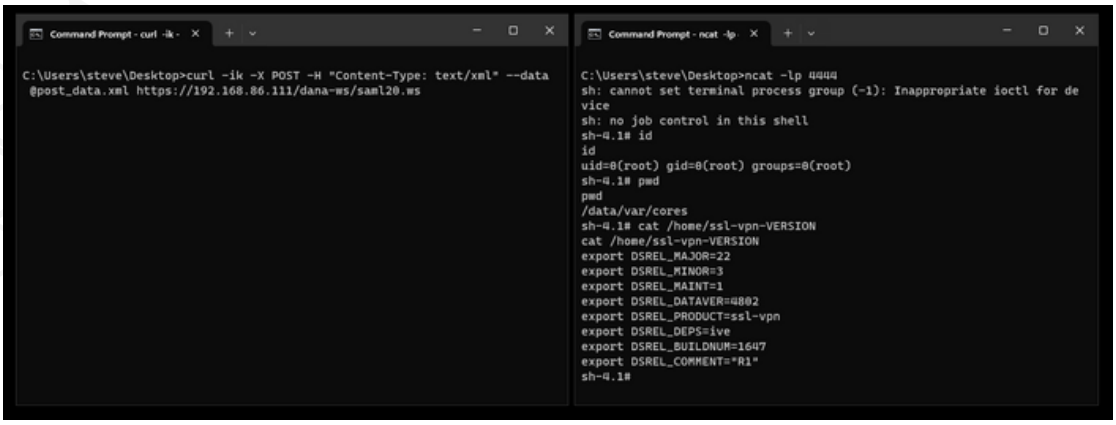
Response and Mitigation:
- Mastodon urges administrators to promptly update servers to secure versions.
- Specific details withheld to allow time for server updates.
- Discovery credited to 'arcaniscanis.'

Recommendation:
- Mastodon server administrators should prioritize updating to secure versions.
- Await further details on the vulnerability's specifics on February 15, 2024, for comprehensive understanding and mitigation.

Acknowledgement:
- Credit to 'arcaniscanis' for discovering the vulnerability.
- Collaboration between Mastodon and the security community in addressing the issue.

https://twitter.com/securestep9/status/1753722560527614412

🌶️ Trending Exploit



https://twitter.com/stephenfewer/status/1753507673742405636

CVE-2024-21893: Server-Side Request Forgery (SSRF) in the Security Assertion Markup Language (SAML) component.

Exploitation through a chain of vulnerabilities: authentication bypass (CVE-2023-46805) and command injection (CVE-2024-21887) leading to unauthenticated remote code execution.

Exploitation Chain:

1. Initial exploitation through authentication bypass and command injection vulnerabilities.
2. New SSRF technique (CVE-2024-21893) discovered to bypass Ivanti's original mitigation.
3. Chaining SSRF to execute arbitrary commands, including Python-based reverse shell payloads.

Mitigation and Remediation:

- Ivanti released a mitigation file addressing CVE-2023-46805 and CVE-2024-21887 before issuing official patches.
- Second mitigation released to prevent both exploit chains.
- Official patches released to address all vulnerabilities.
- Verification by Rapid7 that the second mitigation effectively blocks the described exploit chain.
- Remediation includes applying the second mitigation and installing the official patch.

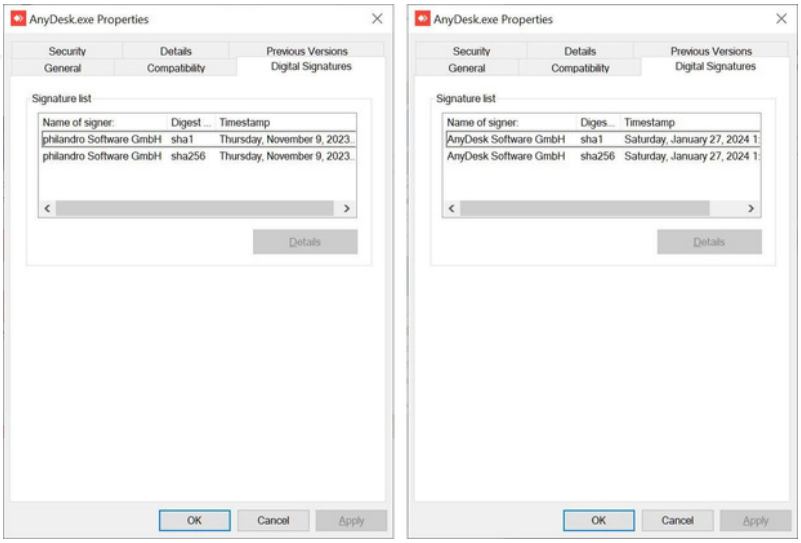
Recommendation:

- Apply the second mitigation provided by Ivanti.
- Install the official patch to address all known vulnerabilities.
- Refer to Ivanti's knowledge base article for detailed guidance on mitigation and patching.

Acknowledgement:

- Credit to security researchers and collaboration between Ivanti and Mandiant in identifying and addressing these vulnerabilities.

The Topic of the Week



https://twitter.com/binitamshah/status/1753745856669663588

AnyDesk, a popular remote access solution used by enterprises worldwide, recently experienced a cyberattack resulting in the theft of source code and private code signing keys. The attack was detected by the company after indications of an incident on their production servers. This report summarizes the incident, AnyDesk's response, and recommendations for users.

Key Points:

1. Attack Details:
   - AnyDesk detected indications of a cyberattack on their production servers and initiated a security audit.
   - Source code and private code signing keys were stolen by threat actors during the attack.
   - The company confirmed that ransomware was not involved in the incident.
2. AnyDesk's Response:
   - AnyDesk engaged cybersecurity firm CrowdStrike to assist in responding to the attack.
   - Security-related certificates were revoked, and affected systems were remediated or replaced.
   - AnyDesk assured customers that their platform was safe to use and that there was no evidence of end-user devices being affected.
   - The company advised users to ensure they are using the latest version of AnyDesk with the new code signing certificate.
   - As a precautionary measure, AnyDesk revoked all passwords to their web portal and recommended users change passwords if reused on other sites.
3. Technical Details:
   - AnyDesk explained that session authentication tokens, crucial for the platform's security, were not stolen during the attack.
   - The company replaced stolen code signing certificates, as indicated in version 8.0.8 released on January 29th.
   - Users are strongly advised to update to the latest version of AnyDesk to ensure continued security.
4. Incident Timeline:
   - AnyDesk suffered a four-day outage starting on January 29th, during which users were unable to log in to the AnyDesk client.
   - Access was restored after maintenance, which was confirmed to be related to the cybersecurity incident.
5. Recommendations for Users:
   - Users should update to the latest version of AnyDesk to benefit from enhanced security measures.
   - Changing passwords for AnyDesk accounts and other platforms where the same password is used is recommended as a precautionary measure.

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.