TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 30TH, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In the dynamic realm of digital advancement, individuals, businesses, and governmental entities are consistently contending with intricate cybersecurity challenges. These issues carry the potential to disrupt regular operations and result in significant financial consequences. It is crucial to strengthen your digital defences and protect your organisation from cyber threats that jeopardise the integrity, confidentiality, and availability of enterprise data.

Enhance your security protocols by incorporating our weekly reports, providing the latest intelligence on cyber threats. Safeguard your IT assets from malicious attacks through our comprehensive advisory services. In an era where digital resilience is of utmost importance, our cyber threat intelligence report empowers your organisation with essential knowledge to bolster your security posture.

GitLab issues critical fix for account hijacking exploit

GitLab has released crucial security updates for both its Community and Enterprise editions, addressing two severe vulnerabilities (CVE-2023-7028 and CVE-2023-5356). The first flaw allows account hijacking without user interaction, posing a significant risk. The second vulnerability involves unauthorised slash command execution through Slack/Mattermost integrations.

Users are strongly advised to promptly update to prevent potential security breaches and supply chain attacks. The authentication issue allows unauthorised password reset requests, even with two-factor authentication (2FA), enabling account takeover and posing a major threat to organisations hosting sensitive data on GitLab. Also, there’s a risk of supply chain attacks when GitLab is used for CI/CD, allowing attackers to insert malicious code into live environments.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	GitLab Community Edition (CE), GitLab Enterprise Edition (EE)

Source - https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-zero-click-account-hijacking-vulnerability/

INTRODUCTION | GITLAB ISSUES FIX | SONICWALL OPEN TO EXPLOITATION | IVANTI FOUND VULNERABLE | PHEMEDRONE STEALER TARGETS WINDOWS | RCE ATTACKS ATLASSIAN CONFLUENCE | REMCOS SPREADS VIA WEBHARD | INDIAN AIR FORCE TARGETED | MALWARE TAKES AIM AT AWS, AZURE, MS | RANSOMWARE EXPLOITS CISCO VPN | RUSSIAN TA ACTIVELY TARGETING NGOS

178K+ SonicWall firewalls open to DoS and RCE exploits

Critical vulnerabilities (CVE-2022-22274 and CVE-2023-0656) have been discovered in SonicWall next-generation firewalls, impacting over 178,000 units and exposing them to denial of service (DoS) and remote code execution (RCE) attacks. This poses a serious security threat, especially considering SonicWall’s extensive user base and past cyberespionage incidents involving the company’s products.

Administrators are strongly advised to secure management interfaces, upgrade firmware, and promptly address the issue. Even if RCE is uncertain, attackers can force appliances into maintenance mode, requiring administrator intervention. With over 500,000 SonicWall firewalls exposed online, including 328,000 in the US, caution is crucial.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	SonicWall

Source - https://www.bleepingcomputer.com/news/security/over-178k-sonicwall-firewalls-vulnerable-to-dos-potential-rce-attacks/

Ivanti warns of active attacks exploiting vulnerabilities in Connect Secure

Global attacks can exploit major flaws in Ivanti VPN and NAC systems, affecting thousands of systems across various organisations, including Fortune 500 companies. The attackers, likely a Chinese state-backed group, has utilised custom malware and advanced techniques to compromise government, military, telecommunications, defence, technology, finance, and aerospace sectors, among others.

This incident is the latest in a series of zero-day exploits targeting Ivanti over several years. While patches are pending, immediate mitigation measures are crucial. Ivanti advises administrators to apply provided mitigations on all ICS VPNs, run the Integrity Checker Tool, and consider compromised data on the VPN appliance if signs of breaches are detected. Shadowserver reports over 16,800 ICS VPN appliances exposed online, with nearly 5,000 in the US.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/ivanti-connect-secure-zero-days-now-under-mass-exploitation/

INTRODUCTION

GITLAB ISSUES FIX

SONICWALL OPEN TO EXPLOITATION

IVANTI FOUND VULNERABLE

PHEMEDRONE STEALER TARGETS WINDOWS

RCE ATTACKS ATLASSIAN CONFLUENCE

REMCOS SPREADS VIA WEBHARD

INDIAN AIR FORCE TARGETED

MALWARE TAKES AIM AT AWS, AZURE, MS

RANSOMWARE EXPLOITS CISCO VPN

RUSSIAN TA ACTIVELY TARGETING NGOS

Phemedrone stealer deployed via Windows flaw

Exploiting a patched vulnerability (CVE-2023-36025) in Microsoft Windows, threat actors (TA) have deployed Phemedrone Stealer, an information-stealing malware targeting web browsers. The malware extracts data from cryptocurrency wallets, Telegram, Steam, and Discord while evading detection by Windows Defender SmartScreen. Despite a November 2023 patch, attackers have persisted in exploiting the vulnerability, highlighting ongoing challenges in countering evolving cyber threats.

The vulnerability affects Windows Defender SmartScreen, allowing TAs to bypass warning checks using crafted Internet Shortcut (.url) files. Although Microsoft issued a patch, the Cybersecurity and Infrastructure Security Agency (CISA) added it to the Known Exploited Vulnerabilities (KEV) list due to evidence of in-the-wild exploitation. Numerous malware campaigns, including Phemedrone Stealer, have incorporated this vulnerability into their attack chains since its disclosure.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.trendmicro.com/en_us/research/24/a/cve-2023-36025-exploited-for-defense-evasion-in-phemedrone-steal.html

INTRODUCTION | GITLAB ISSUES FIX | SONICWALL OPEN TO EXPLOITATION | IVANTI FOUND VULNERABLE | PHEMEDRONE STEALER TARGETS WINDOWS | RCE ATTACKS ATLASSIAN CONFLUENCE | REMCOS SPREADS VIA WEBHARD | INDIAN AIR FORCE TARGETED | MALWARE TAKES AIM AT AWS, AZURE, MS | RANSOMWARE EXPLOITS CISCO VPN | RUSSIAN TA ACTIVELY TARGETING NGOS

Critical RCE vulnerability in Atlassian Confluence datacentre and server

Atlassian Confluence datacentre and server versions released before December 5, 2023, face a critical RCE vulnerability (CVE-2023-22527) due to template injection. This flaw allows unauthorised attackers to execute remote codes. Atlassian has released updates for affected versions, including 8.5.4 (LTS), 8.6.0, and 8.7.1 (datacentre only). Users of unsupported versions, specifically 8.4.5 and earlier, are urged to migrate promptly. Administrators are advised to apply updates to address potential vulnerabilities highlighted in the January security bulletin.

Versions released after December are not affected, and users of unsupported versions are recommended to move to actively supported releases. Atlassian provides no mitigation or workarounds, emphasising the importance of applying available updates. The vulnerability does not impact Confluence LTS v7.19.x, cloud instances hosted by Atlassian, or any other Atlassian product.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Atlassian Confluence

Source - https://www.bleepingcomputer.com/news/security/atlassian-warns-of-critical-rce-flaw-in-older-confluence-versions/

Remcos RAT spreads via WebHard-hosted adult games

Remcos, a remote access trojan (RAT), has been discovered using WebHard to propagate itself in South Korea, disguising as adult-themed games. WebHard, a popular online file storage system in the country, is exploited for distributing this malware. Unlike previous instances involving njRAT and UDP RAT, the AhnLab Security Emergency Response Center (ASEC) found Remcos being delivered through this method.

In these attacks, users are deceived into opening malicious files masquerading as adult games, triggering the execution of harmful Visual Basic scripts, and launching an intermediate binary called “ffmpeg.exe.” This process retrieves the Remcos RAT from a server controlled by TAs. Originally marketed as a legitimate remote administration tool in 2016, Remcos has evolved into a sophisticated tool for unauthorised remote control and surveillance, enabling the exfiltration of sensitive data. It has become a potent weapon used by adversaries to infiltrate systems and establish control.

ATTACK TYPE	Malware	SECTOR	All
REGION	South Korea	APPLICATION	Generic

Source - https://thehackernews.com/2024/01/remcos-rat-spreading-through-adult.html

INTRODUCTION | GITLAB ISSUES FIX | SONICWALL OPEN TO EXPLOITATION | IVANTI FOUND VULNERABLE | PHEMEDRONE STEALER TARGETS WINDOWS | RCE ATTACKS ATLASSIAN CONFLUENCE | REMCOS SPREADS VIA WEBHARD | INDIAN AIR FORCE TARGETED | MALWARE TAKES AIM AT AWS, AZURE, MS | RANSOMWARE EXPLOITS CISCO VPN | RUSSIAN TA ACTIVELY TARGETING NGOS

Cyberattack exploits Slack to steal data from Indian Air Force

A variation of the Go Stealer, masquerading as a ZIP file linked to Indian Air Force aircraft procurement, has emerged, posing a potential threat to Indian defence personnel. The malware displays sophisticated features, such as targeted browser extraction and data exfiltration through Slack. The timing of the attack aligns with the Indian government's fighter jet acquisition announcement, indicating potential espionage or targeted actions.

This variant stands out with added functionalities, including expanded browser targeting and the ability to exfiltrate data through Slack. In contrast to broader-stealing malware, this specific stealer focuses on pilfering login credentials and cookies from four specific browsers, suggesting a tactical approach for acquiring specific sensitive information. Enhanced security measures are crucial in the defence sector considering this threat.

ATTACK TYPE	Malware	SECTOR	Defence
REGION	India	APPLICATION	Windows

Source - https://cyble.com/blog/cyber-espionage-attack-on-the-indian-air-force-go-based-infostealer-exploits-slack-for-data-theft/

INTRODUCTION | GITLAB ISSUES FIX | SONICWALL OPEN TO EXPLOITATION | IVANTI FOUND VULNERABLE | PHEMEDRONE STEALER TARGETS WINDOWS | RCE ATTACKS ATLASSIAN CONFLUENCE | REMCOS SPREADS VIA WEBHARD | INDIAN AIR FORCE TARGETED | MALWARE TAKES AIM AT AWS, AZURE, MS | RANSOMWARE EXPLOITS CISCO VPN | RUSSIAN TA ACTIVELY TARGETING NGOS

AndroxGh0st Malware stealing AWS, Azure, Office 365 accounts

A joint FBI-CISA warning highlights the threat of the Androxgh0st malware, which is actively building a botnet to pilfer cloud credentials (AWS, Microsoft, etc.) from vulnerable Laravel websites. This Python-scripted malware exploits RCE vulnerabilities and misuses simple mail transfer protocol (SMTP) for spam campaigns. Mitigation measures include updating systems, securing Laravel applications, reviewing credentials, scanning files, and monitoring outgoing requests. CISA has added the exploited Laravel vulnerability to its catalogue, urging federal agencies to secure systems by February 6.

The attackers leverage various vulnerabilities, such as CVE-2017-9841 (PHPUnit), CVE-2021-41773 (Apache HTTP Server), and CVE-2018-15133 (Laravel Framework). AndroxGh0st exhibits multiple features for SMTP abuse, including scanning, exploiting exposed credentials and APIs, and deploying web shells. For AWS, the malware scans and parses keys, with the ability to generate keys for brute-force attacks. Compromised AWS credentials are then used to create new users, policies, and instances for malicious scanning activities.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Azure Cloud services, Microsoft Office 365

Source - https://thehackernews.com/2024/01/feds-warn-of-androxgh0st-botnet.html

INTRODUCTION

GITLAB ISSUES FIX

SONICWALL OPEN TO EXPLOITATION

IVANTI FOUND VULNERABLE

PHEMEDRONE STEALER TARGETS WINDOWS

RCE ATTACKS ATLASSIAN CONFLUENCE

REMCOS SPREADS VIA WEBHARD

INDIAN AIR FORCE TARGETED

MALWARE TAKES AIM AT AWS, AZURE, MS

RANSOMWARE EXPLOITS CISCO VPN

RUSSIAN TA ACTIVELY TARGETING NGOS

Medusa ransomware expands arsenal with data leaks and multi-extortion

Since 2022, the Medusa ransomware has escalated its operations, employing a dedicated dark web leak site and a multi-extortion strategy globally. Targeting various industries, Medusa utilises sophisticated tactics, exploiting vulnerabilities and adopting living-off-the-land methods. This aligns with the professionalisation of ransomware, seen in secondary extortion attempts by actors posing as researchers and a rise in Akira ransomware incidents exploiting a Cisco VPN flaw.

Medusa TAs use both an onion site and a public Telegram channel called "information support" for extortion, sharing compromised organisation files. Palo Alto Networks provides protection through Cortex XDR and WildFire Cloud-Delivered Security Services. The Unit 42 Incident Response team is available for assistance in responding to compromises and proactive risk assessments.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/

COLDRIVER deploys custom malware in shift from phishing attacks

The Russian TA, COLDRIVER, previously focused on credential phishing, has advanced its tactics with the creation of custom malware called “SPICA,” cleverly disguised as harmless PDFs. This unique malware targets high-profile individuals among NGOs, governments, and former military officials, allowing for information gathering and remote control. The attack raises concerns about potential intelligence gathering for Russia.

While the number of victims is unknown, COLDRIVER’s evolving tactics emphasise the need for increased vigilance. The group employs spear-phishing campaigns to build trust with victims, utilising bogus sign-in pages to harvest credentials. Microsoft’s analysis highlights the use of server-side scripts to evade automated scanning. Google TAG’s recent findings reveal COLDRIVER’s use of benign PDF documents for enticement since November 2022.

ATTACK TYPE	Malware	SECTOR	Government, education, energy, defence
REGION	UK, US	APPLICATION	Generic

Source - https://thehackernews.com/2024/01/russian-coldriver-hackers-expand-beyond.html

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today’s cyber threat landscape.

Book your visit

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.