27 Fed 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

Articles

New Anubis Ransomware Could Pose Major Threat to Organizations

Threat Intelligence firm Kela warns of a new ransomware group called Anubis operating as a RaaS service with an extensive array of options for affiliates. The group emerged as recently as late 2024, although the researchers believe that its members have experience in ransomware, both malware and operations. Information on Anubis comes from an analysis of the group's dark web footprint rather than code analysis of the ransomware. As with most ransomware groups today, Anubis uses double extortion. The researchers suggest that "Anubis appears to be an emerging threat, highlighting different business models employed by modern extortion actors."

https://www.securityweek.com/new-ransomware-anubis-could-pose-major-threat-to-organizations/

Cisco Patches Vulnerabilities in Nexus Switches

Cisco informed customers on Wednesday that it has patched command injection and denial-of-service (DoS) vulnerabilities in some of its Nexus switches. One of the vulnerabilities, tracked as CVE-2025-20111, has been described as a high-severity issue related to the incorrect handling of some Ethernet frames. The issue impacts the health monitoring diagnostics component of Nexus 3000 and 9000 series switches — in the case of 9000 series products, they are affected only in standalone NX-OS mode. The vulnerability can allow an unauthenticated attacker who has access to the targeted device to cause a DoS condition.

https://www.securityweek.com/cisco-patches-vulnerabilities-in-nexus-switches/

Siemens Teamcenter Vulnerability Could Allow Account Takeover (CVE-2025-23363)

A high-severity vulnerability (CVE-2025-23363) in the Siemens Teamcenter product lifecycle management (PLM) software could allow an attacker to steal users' valid session data and gain unauthorized access to the vulnerable application. CVE-2025-23363 is an open redirect vulnerability in Teamcenter's single sign-on (SSO) login service. In affected applications – currently all versions of Siemens Teamcenter – the service accepts user-controlled input that could specify a link to an external site. This may allow an attacker to craft a link to redirect the legitimate user to an attacker-chosen URL to steal valid session data.

https://www.helpnetsecurity.com/2025/02/27/siemens-teamcenter-vulnerability-could-allow-account-takeover-cve-2025-23363/

PolarEdge Botnet Exploits Cisco and Other Flaws to Hijack ASUS, QNAP, and Synology Devices

A new malware campaign has been observed targeting edge devices from Cisco, ASUS, QNAP, and Synology to rope them into a botnet named PolarEdge since at least the end of 2023. French cybersecurity company Sekoia said it observed the unknown threat actors leveraging CVE-2023-20118 (CVSS score: 6.5), a critical security flaw impacting Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers that could result in arbitrary command execution on susceptible devices. The vulnerability remains unpatched due to the routers reaching end-of-life (EoL) status. As mitigations, Cisco recommended in early 2023 that the flaw be mitigated by disabling remote management and blocking access to ports 443 and 60443.

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

2

https://thehackernews.com/2025/02/polaredge-botnet-exploits-cisco-and.html

Bybit Hack Traced to Safe{Wallet} Supply Chain Attack Exploited by North Korean Hackers

The U.S. Federal Bureau of Investigation (FBI) formally linked the record-breaking $1.5 billion Bybit hack to North Korean threat actors, as the company's CEO Ben Zhou declared a "war against Lazarus." The agency said the Democratic People's Republic of Korea (North Korea) was responsible for the theft of the virtual assets from the cryptocurrency exchange, attributing it to a specific cluster it tracks as TraderTraitor, which is also referred to as Jade Sleet, Slow Pisces, and UNC4899.

https://thehackernews.com/2025/02/bybit-hack-traced-to-safewallet-supply.html

VSCode Extensions with 9 Million Installs Pulled Over Security Risks

Microsoft has removed two popular VSCode extensions, 'Material Theme – Free' and 'Material Theme Icons – Free,' from the Visual Studio Marketplace for allegedly containing malicious code. The two extensions are very popular, having been downloaded nearly 9 million times in total, with users now receiving alerts in VSCode that the extensions have automatically been disabled. The publisher, Mattia Astorino (aka equinusocio), has multiple extensions on the VSCode marketplace, totaling over 13 million installs.

https://www.bleepingcomputer.com/news/security/vscode-extensions-with-9-million-installs-pulled-over-security-risks/

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics DC3 Cyber Crime Center

3