



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

28 Apr 25

Cyber Threat Roundup

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

Contents

Articles	2
New Critical SAP NetWeaver Flaw Exploited to Drop Web Shell, Brute Ratel Framework	2
Critical Commvault RCE Vulnerability Fixed, PoC Available (CVE-2025-34028)	2
North Korean Hackers Spread Malware via Fake Crypto Firms and Job Interview Lures	2
PoC exploit for critical Erlang/OTP SSH bug is public (CVE-2025-32433).....	2
Phishers Exploit Google Sites and DKIM Replay to Send Signed Emails, Steal Credentials	3
Attackers Phish OAuth Codes, Take Over Microsoft 365 Accounts.....	3
Lotus Panda Hacks SE Asian Governments with Browser Stealers and Sideloaded Malware	3
Rack Ruby Vulnerability Could Reveal Secrets to Attackers (CVE-2025-27610).....	3

Articles

New Critical SAP NetWeaver Flaw Exploited to Drop Web Shell, Brute Ratel Framework

Threat actors are likely exploiting a new vulnerability in SAP NetWeaver to upload JSP web shells with the goal of facilitating unauthorized file uploads and code execution. "The exploitation is likely tied to either a previously disclosed vulnerability like CVE-2017-9844 or an unreported remote file inclusion (RFI) issue," ReliaQuest said in a report published this week. The cybersecurity said the possibility of a zero-day stems from the fact that several of the impacted systems were already running the latest patches.

<https://thehackernews.com/2025/04/sap-confirms-critical-netweaver-flaw.html>

Critical Commvault RCE Vulnerability Fixed, PoC Available (CVE-2025-34028)

CVE-2025-34028 is a path traversal vulnerability affecting Commvault Command Center (Innovation Release) versions from 11.38.0 to 11.38.19, on Windows and Linux. It was unearthed by watchTowr researcher Sonny Macdonald, who discovered an endpoint that can be reached without prior authentication, and a server-side request forgery (SSRF) vulnerability and path traversal issues that can be exploited to: Force the vulnerable Commvault instances to fetch a malicious ZIP file from an externally controlled server or unzip the file, execute and trigger the shell within it, thus achieving remote code execution.

<https://www.helpnetsecurity.com/2025/04/24/critical-commvault-rce-vulnerability-fixed-poc-available-cve-2025-34028/>

North Korean Hackers Spread Malware via Fake Crypto Firms and Job Interview Lures

North Korea-linked threat actors behind the Contagious Interview have set up front companies as a way to distribute malware during the fake hiring process. "In this new campaign, the threat actor group is using three front companies in the cryptocurrency consulting industry—BlockNovas LLC (blocknovas[.]com), Angeloper Agency (angeloper[.]com), and SoftGlide LLC (softglide[.]co)—to spread malware via 'job interview lures,' Silent Push said in a deep-dive analysis. The activity, the cybersecurity company said, is being used to distribute three different known malware families, BeaverTail, InvisibleFerret, and OtterCookie.

<https://thehackernews.com/2025/04/north-korean-hackers-spread-malware-via.html>

PoC exploit for critical Erlang/OTP SSH bug is public (CVE-2025-32433)

Erlang/OTP SSH is a set of libraries that allows developers to embed SSH server or client functionality directly into Erlang applications. Erlang/OTP is commonly found in IoT devices and telecommunications platforms/systems. CVE-2025-32433 may allow unauthenticated malicious actors with network access to hosts (computers) running an Erlang/OTP SSH server to execute arbitrary code in the context of the SSH daemon. "If your SSH daemon is running as root, the attacker has full access to your device. Consequently, this vulnerability may lead to full compromise of hosts, allowing for unauthorized access to and manipulation of sensitive data by third parties, or

denial-of-service attacks," Fabian Bäumer, Chair for Network and Data Security at Ruhr University Bochum, explained in a post on the OSS-SEC mailing list last Wednesday.

<https://www.helpnetsecurity.com/2025/04/22/working-poc-exploit-for-critical-erlang-otp-ssh-bug-is-public-cve-2025-32433/>

Phishers Exploit Google Sites and DKIM Replay to Send Signed Emails, Steal Credentials

In what has been described as an "extremely sophisticated phishing attack," threat actors have leveraged an uncommon approach that allowed bogus emails to be sent via Google's infrastructure and redirect message recipients to fraudulent sites that harvest their credentials. "The first thing to note is that this is a valid, signed email – it really was sent from no-reply@google.com," Nick Johnson, the lead developer of the Ethereum Name Service (ENS), said in a series of posts on X. "It passes the DKIM signature check, and Gmail displays it without any warnings – it even puts it in the same conversation as other, legitimate security alerts."

<https://thehackernews.com/2025/04/phishers-exploit-google-sites-and-dkim.html>

Attackers Phish OAuth Codes, Take Over Microsoft 365 Accounts

Suspected Russian threat actors are using OAuth-based phishing attacks to get targets to grant them access to their Microsoft 365 (M365) accounts. "The primary tactics observed involve the attacker requesting victim's supply Microsoft Authorization codes, which grant the attacker with account access to then join attacker-controlled devices to Entra ID (previously Azure AD), and to download emails and other account-related data," according to Volexity researchers. These recently observed attacks rely heavily on one-on-one interaction with a target, as the threat actor must both convince them to click a link and send back a Microsoft-generated code.

<https://www.helpnetsecurity.com/2025/04/23/microsoft-365-oauth-phishing/>

Lotus Panda Hacks SE Asian Governments with Browser Stealers and Sideloaded Malware

The China-linked cyber espionage group tracked as Lotus Panda has been attributed to a campaign that compromised multiple organizations in an unnamed Southeast Asian country between August 2024 and February 2025. "Targets included a government ministry, an air traffic control organization, a telecoms operator, and a construction company," the Symantec Threat Hunter Team said in a new report shared with The Hacker News. "The attacks involved the use of multiple new custom tools, including loaders, credential stealers, and a reverse SSH tool." The intrusion set is also said to have targeted a news agency located in another country in Southeast Asia and an air freight organization located in another neighboring country.

<https://thehackernews.com/2025/04/lotus-panda-hacks-se-asian-governments.html>

Rack Ruby Vulnerability Could Reveal Secrets to Attackers (CVE-2025-27610)

Researchers have uncovered three serious vulnerabilities in Rack, a server interface used by most Ruby web app frameworks (Ruby on Rails, Sinatra, Hanami, Roda, and others). Two of the flaws – CVE-2025-25184 and CVE-

2025-27111 – could allow attackers to manipulate log content and entries, while the third one – CVE-2025-27610 – is a path traversal vulnerability that may allow attackers to gain unauthorized access to sensitive information. Rack provides a standardized way for web servers and Ruby web applications to communicate, and is a core component of many web applications that are used by businesses and consumers. It is available as a Ruby Gem (i.e., reusable package of Ruby code). OPSWAT researchers Thai Do and Minh Pham have found the three vulnerabilities and have singled out CVE-2025-27610 as the most severe.

<https://www.helpnetsecurity.com/2025/04/25/rack-ruby-vulnerability-could-reveal-secrets-to-attackers-cve-2025-27610/>