Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 March 2026

Vulnerabilities

Citrix Urges Patching Critical NetScaler Flaw Allowing Unauthenticated Data Leaks

The Hacker News - 24 March 2026 12:29

Citrix has released security updates to address two vulnerabilities in NetScaler ADC and NetScaler Gateway, including a critical flaw that could be exploited to leak sensitive data from the application.

CISA Orders US Government to Patch Maximum Severity Cisco Flaw

Infosecurity Magazine - 23 March 2026 11:30

CISA added CVE-2026-20131 to its KEV catalog as it is being used in ransomware campaigns

QNAP fixed four vulnerabilities demonstrated at Pwn2Own Ireland 2025

Security Affairs - 23 March 2026 21:49

QNAP fixed four vulnerabilities shown at Pwn2Own 2025 that could enable code execution, data access, or system disruption. Taiwanese vendor QNAP has addressed multiple vulnerabilities, including four SD-WAN router issues (CVE-2025-62843 to CVE-2025-62846) demonstrated at the Pwn2Own Ireland 2025 by Team DDOS.

Hackers Exploit CVE-2025-32975 (CVSS 10.0) to Hijack Unpatched Quest KACE SMA Systems

The Hacker News - 23 March 2026 12:45

Threat actors are suspected to be exploiting a maximum-severity security flaw impacting Quest KACE Systems Management Appliance (SMA), according to Arctic Wolf.The cybersecurity company said it observed malicious activity starting the week of March 9, 2026, in customer environments that's consistent with the exploitation of CVE-2025-32975 on unpatched SMA systems exposed to the internet.

Threat actors and malware

TeamPCP deploys Iran-targeted wiper in Kubernetes attacks

BleepingComputer - 23 March 2026 17:09

The TeamPCP hacking group is targeting Kubernetes clusters with a malicious script that wipes all machines when it detects systems configured for Iran. [...]

Trivy supply-chain attack spreads to Docker, GitHub repos

BleepingComputer - 23 March 2026 14:40

The TeamPCP hackers behind the Trivy supply-chain attack continued to target Aqua Security, pushing malicious Docker images and hijacking the company's GitHub organization to tamper with dozens of repositories. [...]

North Korea-linked threat actors abuse VS Code auto-run to spread StoatWaffle malware

Security Affairs - 24 March 2026 08:09

North Korea-linked threat actors use VS Code auto-run tasks to spread StoatWaffle malware via malicious projects that execute on folder open.

Pro-Iranian Nasir Security is targeting energy companies in the Gulf

Security Affairs - 23 March 2026 15:39

Resecurity tracks Iran-linked Nasir Security targeting Middle East energy firms amid ongoing regional cyber and military threats. Resecurity (USA) is tracking a relatively new cybercriminal group called Nasir Security, presumably associated with Iran, that is targeting energy organizations in the Middle East.

Iran-linked actors use Telegram as C2 in malware attacks on dissidents

Security Affairs - 23 March 2026 10:35

Iran-linked actors use Telegram as C2 to spread malware targeting dissidents and journalists, enabling surveillance and data theft. The FBI warns that Iran's Ministry of Intelligence and Security (MOIS) runs cyber campaigns using Telegram as a command-and-control infrastructure to deliver malware.

Microsoft Warns IRS Phishing Hits 29,000 Users, Deploys RMM Malware

The Hacker News - 23 March 2026 17:25

Microsoft has warned of fresh campaigns that are capitalizing on the upcoming tax season in the U.S. to harvest credentials and deliver malware.The email campaigns take advantage of the urgency and time-sensitive nature of emails to send phishing messages masquerading as refund notices, payroll forms, filing reminders, and requests from tax professionals to deceive recipients into opening

Ransomware's New Era: Moving at AI Speed

darkreading - 23 March 2026 22:40

Threat actors bypass security tools and use AI to launch faster ransomware attacks that exploit valid credentials and target data