Scottish Cyber Coordination Centre

Daily threat bulletin

6 June 2024

Vulnerabilities

Cisco addressed Webex flaws used to compromise German government meetings

Security Affairs - 05 June 2024 14:37

Cisco addressed vulnerabilities that were exploited to compromise the Webex meetings of the German government. In early May, German media outlet Zeit Online revealed that threat actors exploited vulnerabilities in the German government's implementation of the Cisco Webex software to access internal meetings.

Zyxel Releases Patches for Firmware Vulnerabilities in EoL NAS Models

The Hacker News - 05 June 2024 13:40

Zyxel has released security updates to address critical flaws impacting two of its network-attached storage (NAS) devices that have currently reached end-of-life (EoL) status. Successful exploitation of three of the five vulnerabilities could permit an unauthenticated attacker to execute operating system (OS) commands and arbitrary code on affected installations.

RansomHub Actors Exploit ZeroLogon Vuln in Recent Ransomware Attacks

darkreading - 05 June 2024 22:24

CVE-2020-1472 is a privilege escalation flaw that allows an attacker to take over an organization's domain controllers.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2017-3506 Oracle WebLogic Server OS Command Injection Vulnerability.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-24919 Check Point Quantum Security Gateways.

Threat actors and malware

Linux version of TargetCompany ransomware focuses on VMware ESXi

BleepingComputer - 05 June 2024 20:17

Researchers observed a new Linux variant of the TargetCompany ransomware family that targets VMware ESXi environments using a custom shell script to deliver and execute payloads. [...]

Qilin ransomware gang linked to attack on London hospitals

BleepingComputer - 05 June 2024 14:57

A ransomware attack that hit pathology services provider Synnovis on Monday and impacted several major NHS hospitals in London has now been linked to the Qilin ransomware operation.

Malware can steal data collected by the Windows Recall tool, experts warn

Security Affairs - 05 June 2024 22:10

Cybersecurity researchers demonstrated how malware could potentially steal data collected by the new Windows Recall tool. The Recall feature of Microsoft Copilot+ is an AI-powered tool designed to help users search for past activities on their PC. The data collected by the tool is stored and processed locally.

RansomHub Rides High on Knight Ransomware Source Code

Security Boulevard - 05 June 2024 20:24

RansomHub, which has become among the most prolific ransomware groups over the past few months, likely got its start with the source code from the Knight malware and a boost from a one-time BlackCat affiliate.

Chinese State-Sponsored Operation “Crimson Palace” Revealed

Infosecurity Magazine - 05 June 2024 17:15

Sophos said the campaign aimed to maintain prolonged network access for espionage purposes.