Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

26 January 2024

Vulnerabilities

Critical Cisco Unified Communications RCE Bug Allows Root Access

Dark Reading - January 25 2024

A critical security vulnerability in Cisco Unified Communications and Contact Center Solutions (UC/CC) could allow unauthenticated remote code execution (RCE). The bug (CVE-2024-20253, 9.9 CVSS) arises thanks to "improper processing of user-provided data that is being read into memory," according to Cisco's advisory, issued yesterday. Remote attackers who are not logged onto the system can simply send specially crafted messages to a vulnerable device's listening port in order to achieve RCE; from there, they can execute code on the underlying operating system with the privileges of the Web services user, and/or gain root access. Cisco's UC/CC platforms are used by small and midsized businesses (SMBs) and enterprises to provide communications over IP, including voice calling, video calls.

Cisco Releases Security Advisory for Multiple Unified Communications and Contact Center Solutions Products

CISA Current Activity - January 25 2024

Cisco released a security advisory to address a vulnerability (CVE-2024-20253) affecting multiple Unified Communications Products. A cyber threat actor could exploit this vulnerability to take control of an affected system. CISA encourages users and administrators to review the Cisco Unified Communications Products Remote Code Execution Vulnerability advisory and apply the necessary updates.

CISA Releases Two Industrial Control Systems Advisories

CISA Current Activity - January 25 2024

CISA released two Industrial Control Systems (ICS) advisories on January 25, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-025-01 Opteev MachineSense FeverWarn ICSA-24-025-02 SystemK NVR 504/508/516 CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

Hackers target WordPress database plugin active on 1 million sites

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Bleeping Computer - January 25 2024

Malicious activity targeting a critical severity flaw in the 'Better Search Replace' WordPress plugin has been detected, with researchers observing thousands of attempts in the past 24 hours.

Ransomware

Annual GRIT Ransomware Report – 2023

Security Boulevard - RSS - January 25 2024

With the conclusion of 2023, the GuidePoint Research and Intelligence Team (GRIT) has compiled our second annual report on ransomware [...] The post Annual GRIT Ransomware Report – 2023 appeared first on Security Boulevard.

Dragos Industrial Ransomware Analysis: Q4 2023

Dragos Blog - RSS - January 25 2024

While international law enforcement's relentless efforts have resulted in arrests and the dismantling of ransomware operations, the battle against ransomware groups continues unabated. During the fourth quarter of 2023, we witnessed a slight decline in reported incidents yet saw a surge in actions that kept the ransomware threat landscape dynamic.

What makes ransomware victims less likely to pay up?

Help Net Security - January 26 2024

There's a good reason why ransomware gangs started exfiltrating victims' data instead of just encrypting it: those organizations pay more. University of Twente researcher Tom Meurs and his colleagues wanted to know which factors influence victims to pay.

Malware and threat actors

'Midnight Blizzard' Breached HPE Email Months Before Microsoft Hack

Dark Reading - January 25 2024

The Russian APT behind the SolarWinds attacks exfiltrated data from HPE email accounts last May.

Microsoft Warns of Widening APT29 Espionage Attacks Targeting Global Orgs

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

The Hacker News - January 26 2024

Microsoft on Thursday said the Russian state-sponsored threat actors responsible for a cyber attack on its systems in late November 2023 have been targeting other organizations and that it's currently beginning to notify them.