Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

19 February 2024

Vulnerabilities

SolarWinds fixes critical RCE bugs in access rights audit solution

Bleeping Computer - February 16 2024

SolarWinds has patched five remote code execution (RCE) flaws in its Access Rights Manager (ARM) solution, including three critical severity vulnerabilities that allow unauthenticated exploitation. Access Rights Manager allows companies to manage and audit access rights across their IT infrastructure to minimize insider threat impact and more. CVE-2024-23476 and CVE-2024-23479 are due to path traversal weaknesses, while the third critical flaw tracked as CVE-2023-40057 is caused by deserialization of untrusted data.

CISA: Cisco ASA/FTD bug CVE-2020-3259 exploited in ransomware attacks

Security Affairs - February 17 2024

CISA warns that the Akira Ransomware gang is exploiting the Cisco ASA/FTD vulnerability CVE-2020-3259 (CVSS score: 7.5) in attacks in the wild. This week the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Cisco ASA and FTD bug, tracked as CVE-2020-3259 (CVSS score: 7.5), to its Known Exploited Vulnerabilities catalog.

ESET fixed high-severity local privilege escalation bug in Windows products

Security Affairs - February 18 2024

Cybersecurity firm ESET has addressed a high-severity elevation of privilege vulnerability in its Windows security solution. ESET addressed a high-severity vulnerability, tracked as CVE-2024-0353 (CVSS score 7.8), in its Windows products. The vulnerability is a local privilege escalation issue that was submitted to the company by the Zero Day Initiative (ZDI).

Malware and threat actors

Week in review: AnyDesk phishing campaign targets employees, Microsoft fixes exploited zero-days

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Help Net Security - February 18 2024

Here's an overview of some of last week's most interesting news, articles, interviews and videos.

Feds post $15 million bounty for info on ALPHV/Blackcat ransomware crew

The Register - Security - February 19 2024

ALSO: EncroChat crims still getting busted; ransomware takes down CO public defenders office; and crit vulns infosec in brief The US government is offering bounties up to $15 million as a reward for anyone willing to help it take out the APLHV/Blackcat ransomware gang.

Russian APT 'Winter Vivern' Targets European Government, Military

Dark Reading - February 17 2024

The Russia-aligned threat group known as Winter Vivern was discovered exploiting cross-site scripting (XSS) vulnerabilities in Roundcube webmail servers across Europe in October — and now its victims are coming to light. The group mainly targeted government, military, and national infrastructure in Georgia, Poland, and Ukraine, according to Recorded Future's Insikt Group report on the campaign released today.