Scottish
Cyber
Coordination
Centre

Daily threat bulletin

22 July 2024

Vulnerabilities

Cisco fixed a critical flaw in Security Email Gateway that could allow attackers to add root users

Security Affairs - 19 July 2024 09:34

Cisco has addressed a critical vulnerability that could allow attackers to add new root users to Security Email Gateway (SEG) appliances. Cisco fixed a critical vulnerability, tracked as CVE-2024-20401 (CVSS score 9.8), that could allow unauthenticated, remote attackers to add new users with root privileges and permanently crash Security Email Gateway (SEG) appliances.

SolarWinds Patches 8 Critical Flaws in Access Rights Manager Software

The Hacker News - 19 July 2024 13:43

SolarWinds has addressed a set of critical security flaws impacting its Access Rights Manager (ARM) software that could be exploited to access sensitive information or execute arbitrary code.Of the 13 vulnerabilities, eight are rated Critical in severity and carry a CVSS score of 9.6 out of 10.0.

Recent Splunk Enterprise Vulnerability Easy to Exploit: Security Firm

SecurityWeek - 19 July 2024 15:43

SonicWall warns that a simple GET request is enough to exploit a recent Splunk Enterprise vulnerability.

Several Linux Kernel Azure Vulnerabilities Fixed in Ubuntu

Security Boulevard - 20 July 2024 10:00

Recently, Canonical released security updates to address several vulnerabilities in the Linux kernel for Microsoft Azure Cloud systems in Ubuntu 16.04 ESM and Ubuntu 18.04 ESM. An attacker could possibly use these issues to cause a denial of service, expose sensitive information, or execute arbitrary code.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2024-34102 Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability, CVE-2024-28995 SolarWinds Serv-U Path Traversal Vulnerability, and CVE-2022-22948 VMware vCenter Server Incorrect Default File Permissions Vulnerability.

Threat actors and malware

Cybercriminals Exploit CrowdStrike Update Mishap to Distribute Remcos RAT Malware

The Hacker News - 20 July 2024 22:31

Cybersecurity firm CrowdStrike, which is facing the heat for causing worldwide IT disruptions by pushing out a flawed update to Windows devices, is now warning that threat actors are exploiting the situation to distribute Remcos RAT to its customers in Latin America under the guise of providing a hotfix.

SocGholish Malware Exploits BOINC Project for Covert Cyberattacks

The Hacker News - 22 July 2024 13:15

The JavaScript downloader malware known as SocGholish (aka FakeUpdates) is being used to deliver a remote access trojan called AsyncRAT as well as a legitimate open-source project called BOINC.BOINC, short for Berkeley Open Infrastructure Network Computing Client, is an open-source “volunteer computing” platform maintained by the University of California.

New Play Ransomware Linux Variant Targets ESXi Shows Ties With Prolific Puma

Cyware News - Latest Cyber News - 20 July 2024 01:00

The Play ransomware group has introduced a Linux variant that targets ESXi environments. This variant verifies its environment before executing and has been successful in evading security measures.

Security Affairs Malware Newsletter Round 3

Security Affairs - 21 July 2024 14:31

Security Affairs Malware newsletter includes a collection of the best articles and research on malware in the international landscape.

UK related

UK arrests suspected Scattered Spider hacker linked to MGM attack

BleepingComputer - 20 July 2024 16:05

UKpolice have arrested a 17-year-old boy suspected of being involved in the 2023 MGM Resorts ransomware attack and a member of the Scattered Spider hacking collective.