Scottish Cyber Coordination Centre

Daily threat bulletin

3 December 2024

Vulnerabilities

Critical Vulnerability Found in Zabbix Network Monitoring Tool

SecurityWeek - 02 December 2024 13:19

A critical-severity vulnerability in open source enterprise network monitoring tool Zabbix could lead to full system compromise.

BootKitty UEFI malware exploits LogoFAIL to infect Linux systems

BleepingComputer - 02 December 2024 14:07

The recently uncovered 'Bootkitty' UEFI bootkit, the first malware of its kind targeting Linux systems, exploits CVE-2023-40238, aka 'LogoFAIL,' to infect computers running on a vulnerable UEFI firmware. [...]

Threat actors and malware

Horns&Hooves Campaign Delivers RATs via Fake Emails and JavaScript Payloads

The Hacker News - 03 December 2024 11:53

A newly discovered malware campaign has been found to target private users, retailers, and service businesses mainly located in Russia to deliver NetSupport RAT and BurnsRAT.The campaign, dubbed Horns&Hooves by Kaspersky, has hit more than 1,000 victims since it began around March 2023. The end goal of these attacks is to leverage the access afforded by these trojans to install stealer

SmokeLoader Malware Campaign Targets Companies in Taiwan

Infosecurity Magazine - 02 December 2024 15:00

SmokeLoader malware identified targeting Taiwanese firms via phishing, exploiting Microsoft Office vulnerabilities

Corrupted Word Files Fuel Sophisticated Phishing Campaign

Infosecurity Magazine - 02 December 2024 17:30

A new phishing attack uses corrupted Word docs to bypass security, luring victims with fake payroll and HR emails

UK cyber chief warns country is 'widely underestimating' risks from cyberattacks

The Record from Recorded Future News - 03 December 2024 01:00

Scottish Cyber Coordination Centre

UK related

Two UK Hospitals Hit by Cyberattacks, One Postponed Procedures

SecurityWeek - 02 December 2024 12:51

Alder Hey Children's Hospital and Wirral University Teaching Hospital have fallen victim to cyberattacks, including one involving ransomware.