Scottish Cyber Coordination Centre

Daily threat bulletin

22 October 2024

Vulnerabilities

Hackers exploit Roundcube webmail flaw to steal email, credentials

BleepingComputer - 21 October 2024 18:14

Threat actors have been exploiting a vulnerability in the Roundcube Webmail client to target government organizations in the Commonwealth of Independent States (CIS) region, the successor of the former Soviet Union. [...]

CISA Adds ScienceLogic SL1 Vulnerability to Exploited Catalog After Active Zero-Day Attack

The Hacker News - 22 October 2024 11:17

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a critical security flaw impacting ScienceLogic SL1 to its Known Exploited Vulnerabilities (KEV) catalog, following reports of active exploitation as a zero-day.

SolarWinds Help Desk software vulnerability added to CISA catalogue

Security Magazine - 21 October 2024 11:00

Due to evidence of active exploitation, CISA added three vulnerabilities to its Known Exploited Vulnerabilities Catalogue.

Threat actors and malware

Over 6,000 WordPress hacked to install plugins pushing infostealers

BleepingComputer - 21 October 2024 14:53

WordPress sites are being hacked to install malicious plugins that display fake software updates and errors to push information-stealing malware. [...]

Bumblebee malware returns after recent law enforcement disruption

BleepingComputer - 21 October 2024 12:45

The Bumblebee malware loader has been spotted in new attacks recently, more than four months after Europol disrupted it during 'Operation Endgame' in May. [...]

Pixel perfect Ghostpulse malware loader hides inside PNG image files

The Register - 22 October 2024 06:30

Miscreants combine it with an equally tricky piece of social engineering The Ghostpulse malware strain now retrieves its main payload via a PNG image file's pixels. This development,

security experts say, is “one of the most significant changes” made by the crooks behind it since launching in 2023....

Chinese Nation-State Hackers APT41 Hit Gambling Sector for Financial Gain

The Hacker News - 21 October 2024 19:38

The prolific Chinese nation-state actor known as APT41 (aka Brass Typhoon, Earth Baku, Wicked Panda, or Winnti) has been attributed to a sophisticated cyber attack targeting the gambling and gaming industry.

Cisco states that data published on cybercrime forum was taken from public-facing DevHub environment

Security Affairs - 21 October 2024 19:39

Cisco confirms that data published by IntelBroker on a cybercrime forum was taken from the company DevHub environment. Cisco confirms that the data posted by the notorious threat actor IntelBroker on a cybercrime forum was stolen from its DevHub environment.