Scottish Cyber Coordination Centre

Daily threat bulletin

4 June 2024

Vulnerabilities

Exploit for critical Progress Telerik auth bypass released, patch now

BleepingComputer - 03 June 2024 14:58

Researchers have published a proof-of-concept (PoC) exploit script demonstrating a chained remote code execution (RCE) vulnerability on Progress Telerik Report Servers. [...]

Multiple flaws in Cox modems could have impacted millions of devices

Security Affairs - 04 June 2024 07:59

Researcher discovered several authorization bypass vulnerabilities in Cox modems that potentially impacted millions of devices.

Oracle WebLogic Server OS Command Injection Flaw Under Active Attack

The Hacker News - 04 June 2024 09:55

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added a security flaw impacting the Oracle WebLogic Server to the Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Atlassian Confluence High-Severity Bug Allows Code Execution

darkreading - 03 June 2024 22:00

Because of the role the Confluence Server plays in managing documentation and knowledge data bases, the researchers recommend users upgrade to patch CVE-2024-21683 as soon as possible.

Check Point warns customers to patch VPN vulnerability under active exploitation

The Register - 03 June 2024 13:02

Also, free pianos are the latest internet scam bait, Cooler Master gets pwned, and some critical vulnerabilities Infosec in brief Cybersecurity software vendor Check Point is warning customers to update their software immediately in light of a zero day vulnerability under active exploitation....

Threat actors and malware

APT28 targets key networks in Europe with HeadLace malware

Security Affairs - 03 June 2024 10:55

Scottish Cyber Coordination Centre

Russia-linked APT28 used the HeadLace malware and credential-harvesting web pages in attacks against networks across Europe. Researchers at Insikt Group observed Russian GRU's unit APT28 targeting networks across Europe with information-stealer Headlace and credential-harvesting web pages.

DarkGate Malware Replaces AutoIt with AutoHotkey in Latest Cyber Attacks

The Hacker News - 04 June 2024 13:03

Cyber attacks involving the DarkGate malware-as-a-service (MaaS) operation have shifted away from AutoIt scripts to an AutoHotkey mechanism to deliver the last stages, underscoring continued efforts on the part of the threat actors to continuously stay ahead of the detection curve.

Researchers Uncover RAT-Dropping npm Package Targeting Gulp Users

The Hacker News - 03 June 2024 20:30

Cybersecurity researchers have uncovered a new suspicious package uploaded to the npm package registry that's designed to drop a remote access trojan (RAT) on compromised systems.

Beware: Fake Browser Updates Deliver BitRAT and Lumma Stealer Malware

The Hacker News - 03 June 2024 10:21

Fake web browser updates are being used to deliver remote access trojans (RATs) and information stealer malware such as BitRAT and Lumma Stealer (aka LummaC2).

Russia Aims Cyber Operations at Summer Olympics

darkreading - 03 June 2024 21:47

As always, Russian APTs are hoping to foment unrest by stoking existing societal divides and fears, this time around the Olympics and EU politics; and, concerns remain around physical disruption.

Europol's Hunt Begins for Emotet Malware Mastermind

darkreading - 03 June 2024 20:48

International law enforcement Operation Endgame shifts its crackdown to focus on individual adversaries.