Scottish Cyber Coordination Centre

Daily threat bulletin

15 August 2024

Vulnerabilities

SolarWinds fixes critical RCE bug affecting all Web Help Desk versions

BleepingComputer - 14 August 2024 12:22

A critical vulnerability in SolarWinds' Web Help Desk solution for customer support could be exploited to achieve remote code execution, the American business software developer warns in a security advisory today. [...]

Fortinet, Zoom Patch Multiple Vulnerabilities

SecurityWeek - 14 August 2024 12:14

Fortinet and Zoom have released patches for multiple vulnerabilities in their products, including high-severity bugs.

Chipmaker Patch Tuesday: Intel, AMD Address Over 110 Vulnerabilities

SecurityWeek - 14 August 2024 11:53

Intel and AMD have each informed customers about dozens of vulnerabilities found and patched in their products. The post Chipmaker Patch Tuesday: Intel, AMD Address Over 110 Vulnerabilities appeared first on SecurityWeek.

Research Uncovers New Microsoft Outlook Vulnerability

Infosecurity Magazine - 14 August 2024 16:00

CVE-2024-38173 is a medium severity RCE flaw in Microsoft Outlook, similar to CVE-2024-30103

Threat actors and malware

New Gafgyt Botnet Variant Targets Weak SSH Passwords for GPU Crypto Mining

The Hacker News - 15 August 2024 11:42

Cybersecurity researchers have discovered a new variant of the Gafgyt botnet that's targeting machines with weak SSH passwords to ultimately mine cryptocurrency on compromised instances using their GPU computational power. This indicates that the "IoT botnet is targeting more robust servers running on cloud native environments," Aqua Security researcher Assaf Morag said in a Wednesday analysis.

Black Basta-Linked Attackers Target Users with SystemBC Malware

The Hacker News - 14 August 2024 23:43

Scottish Cyber Coordination Centre

An ongoing social engineering campaign with alleged links to the Black Basta ransomware group has been linked to “multiple intrusion attempts” with the goal of conducting credential theft and deploying a malware dropper called SystemBC.

Inc Ransomware Encryptor Contains Keys to Victim Data Recovery

darkreading - 14 August 2024 11:00

The threat group is disrupting healthcare organizations. Victims can help themselves, though, even after compromise, by being careful in the decryption process.

New Phishing Attack Uses Sophisticated Infostealer Malware

Infosecurity Magazine - 14 August 2024 17:00

The phishing attack uses infostealer malware to target saved passwords, credit cards & Bitcoin info

UK related

Cyber-Attack Spreads Phishing Scam Across Greater Manchester Areas

Infosecurity Magazine - 14 August 2024 11:30

A cyber-attack has hit several boroughs across Greater Manchester, England, leaving thousands of residents vulnerable to a phishing scam.

NCSC Calls on UK Firms to Join Mass Cyber-Deception Initiative

Infosecurity Magazine - 14 August 2024 10:30

The UK’s National Cyber Security Centre wants to test the effectiveness of cyber-deception tactics.