Scottish Cyber Coordination Centre

Daily threat bulletin

15 May 2024

Vulnerabilities

PoC exploit released for RCE zero-day in D-Link EXO AX4800 routers

BleepingComputer - 14 May 2024 19:10

The D-Link EXO AX4800 (DIR-X4860) router is vulnerable to remote unauthenticated command execution that could lead to complete device takeovers by attackers with access to the HNAP port. [...]

Apple fixes Safari WebKit zero-day flaw exploited at Pwn2Own

BleepingComputer - 14 May 2024 12:56

Apple has released security updates to fix a zero-day vulnerability in the Safari web browser exploited during this year's Pwn2Own Vancouver hacking competition. [...]

Microsoft Patch Tuesday security updates for May 2024 fixes 2 actively exploited zero-days

Security Affairs - 14 May 2024 22:17

Microsoft Patch Tuesday security updates for May 2024 fixed 59 flaws across various products including an actively exploited zero-day.

VMware Patches Severe Security Flaws in Workstation and Fusion Products

The Hacker News - 14 May 2024 22:19

Multiple security flaws have been disclosed in VMware Workstation and Fusion products that could be exploited by threat actors to access sensitive information, trigger a denial-of-service (DoS) condition, and execute code under certain circumstances.

Critical Flaws in Cacti Framework Could Let Attackers Execute Malicious Code

The Hacker News - 14 May 2024 17:47

The maintainers of the Cacti open-source network monitoring and fault management framework have addressed a dozen security flaws, including two critical issues that could lead to the execution of arbitrary code.

Adobe Patches Critical Flaws in Reader, Acrobat

SecurityWeek - 14 May 2024 18:05

Adobe documents multiple code execution flaws in a wide range of products, including the widely deployed Adobe Acrobat and Reader software.

Scottish Cyber Coordination Centre

Threat actors and malware

Top 5 Most Dangerous Cyber Threats in 2024

darkreading - 15 May 2024 00:43

SANS Institute experts weigh in on the top threat vectors faced by enterprises and the public at large.

Ebury botnet malware infected 400,000 Linux servers since 2009

BleepingComputer - 14 May 2024 13:31

A malware botnet known as 'Ebury' has infected almost 400,000 Linux servers since 2009, with roughly 100,000 still compromised as of late 2023. [...]

Phorpiex botnet sent millions of phishing emails to deliver LockBit Black ransomware

Security Affairs - 14 May 2024 07:57

Experts reported that since April, the Phorpiex botnet sent millions of phishing emails to spread LockBit Black ransomware. New Jersey's Cybersecurity and Communications Integration Cell (NJCCIC) reported that since April, threat actors used the the Phorpiex botnet to send millions of phishing emails as part of a LockBit Black ransomware campaign.

As the FBI Closes In, Scattered Spider Attacks Finance, Insurance Orgs

darkreading - 14 May 2024 21:18

Scattered Spider is as active as ever, despite authorities claiming that they're close to nailing its members.

Russian Actors Weaponize Legitimate Services in Multi-Malware Attack

Infosecurity Magazine - 14 May 2024 15:00

Recorded Future details a novel campaign that abuses legitimate internet services to deploy multiple malware variants for credential theft

UK Insurance and NCSC Join Forces to Fight Ransomware Payments

Infosecurity Magazine - 14 May 2024 12:00

UK insurers and the National Cybersecurity Centre release new guidance to discourage ransomware payments by businesses