Scottish Cyber Coordination Centre

Daily threat bulletin

22 April 2024

Vulnerabilities

Critical Forminator plugin flaw impacts over 300k WordPress sites

BleepingComputer - 20 April 2024 12:19

The Forminator WordPress plugin used in over 500,000 sites is vulnerable to a flaw that allows malicious actors to perform unrestricted file uploads to the server. [...]

CrushFTP warns users to patch exploited zero-day “immediately”

BleepingComputer - 19 April 2024 19:33

CrushFTP warned customers today in a private memo of an actively exploited zero-day vulnerability fixed in new versions released today, urging them to patch their servers immediately. [...]

MITRE revealed that nation-state actors breached its systems via Ivanti zero-days

Security Affairs - 19 April 2024 22:54

The MITRE Corporation revealed that a nation-state actor compromised its systems in January 2024 by exploiting Ivanti VPN zero-days. In April 2024, MITRE disclosed a security breach in one of its research and prototyping networks. The security team at the organization promptly launched an investigation, logged out the threat actor, and engaged third-party forensics Incident [...]

Palo Alto Networks Discloses More Details on Critical PAN-OS Flaw Under Attack

The Hacker News - 20 April 2024 12:23

Palo Alto Networks has shared more details of a critical security flaw impacting PAN-OS that has come under active exploitation in the wild by malicious actors.The company described the vulnerability, tracked as CVE-2024-3400 (CVSS score: 10.0), as “intricate” and a combination of two bugs in versions PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 of the software.”In

Scottish Cyber Coordination Centre

Threat actors and malware

HelloKitty ransomware rebrands, releases CD Projekt and Cisco data

BleepingComputer - 19 April 2024 16:20

An operator of the HelloKitty ransomware operation announced they changed the name to 'HelloGookie,' releasing passwords for previously leaked CD Projekt source code, Cisco network information, and decryption keys from old attacks.. [...]

BlackTech Targets Tech, Research, and Gov Sectors New 'Deuterbear' Tool

The Hacker News - 19 April 2024 20:14

Technology, research, and government sectors in the Asia-Pacific region have been targeted by a threat actor called BlackTech as part of a recent cyber attack wave.The intrusions pave the way for an updated version of modular backdoor dubbed Waterbear as well as its enhanced successor referred to as Deuterbear."Waterbear is known for its complexity, as it

LabHost Phishing Platform is Latest Target of International Law Agencies

Security Boulevard - 19 April 2024 20:46

The takedown this week of a massive phishing-as-a-service (PhaaS) operation spanned law enforcement agencies from both sides of the Atlantic and is the latest example of an increasingly aggressive approach by authorities to disrupt the operations of high-profile cybercriminal gangs. Agencies from 19 countries participated in the operation against the LabHost, which first appeared in..The post LabHost Phishing Platform is Latest Target of International Law Agencies appeared first on Security Boulevard.

SafeBreach Coverage for AA24-109A (Akira Ransomware)

Security Boulevard - 19 April 2024 19:56

FBI, CISA, EC3, and NCSC-NL issued an urgent advisory highlighting the use of new TTPs and IOCs by the Akira ransomware group.The post SafeBreach Coverage for AA24-109A (Akira Ransomware) appeared first on SafeBreach.The post SafeBreach Coverage for AA24-109A (Akira Ransomware) appeared first on Security Boulevard.

MITRE admits 'nation state' attackers touched its NERVE R&D operation

The Register - 22 April 2024 02:57

PLUS: Akira ransomware resurgent; Telehealth outfit fined for data-sharing; This week's nastiest vulns Infosec In Brief In a cautionary tale that no one is immune from attack, the security org MITRE has admitted that it got pwned....

CISA and Partners Release Advisory on Akira Ransomware

Scottish Cyber Coordination Centre

CISA Advisories -

Today, CISA, the Federal Bureau of Investigation (FBI), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Akira Ransomware, to disseminate known Akira ransomware tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as February 2024.Evolving from an initial focus on Windows systems to a Linux variant targeting VMware ESXi virtual machines, Akira threat actors began deploying Megazord (a Rust-based code) and Akira (written in C++), including Akira_v2 (also Rust-based) in August 2023. Akira ransomware has impacted a wide range of businesses and critical infrastructure entities in North America, Europe, and Australia and claimed approximately $42 million (USD) in ransomware proceeds.CISA and partners encourage critical infrastructure organizations to review and implement the mitigations provided in the joint CSA to reduce the likelihood and impact of Akira and other ransomware incidents. For more information, see CISA's #StopRansomware webpage and the updated #StopRansomware Guide.