Scottish Cyber Coordination Centre

Daily threat bulletin

19 April 2024

Vulnerabilities

ICS Network Controllers Open to Remote Exploit, No Patches Available

darkreading - 18 April 2024 21:25

CISA advisory warns of critical ICS device flaws, but a lack of available fixes leaves network administrators on defense to prevent exploits.

Cisco Says PoC Exploit Available for Newly Patched IMC Vulnerability

SecurityWeek - 18 April 2024 12:42

Cisco patches a high-severity Integrated Management Controller vulnerability for which PoC exploit code is available.The post Cisco Says PoC Exploit Available for Newly Patched IMC Vulnerability appeared first on SecurityWeek.

New Cyber-Threat MadMxShell Exploits Typosquatting and Google Ads

Infosecurity Magazine - 18 April 2024 16:30

Zscaler also confirmed MadMxShell uses DLL sideloading and DNS tunneling for C2 communication

Threat actors and malware

Previously unknown Kapeka backdoor linked to Russian Sandworm APT

Security Affairs - 18 April 2024 10:39

Russia-linked APT Sandworm employed a previously undocumented backdoor called Kapeka in attacks against Eastern Europe since 2022. WithSecure researchers identified a new backdoor named Kapeka that has been used in attacks targeting victims in Eastern Europe since at least mid-2022. The backdoor is very sophisticated, it serves as both an initial toolkit and as a backdoor.

Hackers Target Middle East Governments with Evasive “CR4T” Backdoor

The Hacker News - 19 April 2024 12:46

Scottish Cyber Coordination Centre

Government entities in the Middle East have been targeted as part of a previously undocumented campaign to deliver a new backdoor dubbed CR4T.Russian cybersecurity company Kaspersky said it discovered the activity in February 2024 with evidence suggesting that it may have been active since at least a year prior.

Evil XDR: Researcher Turns Palo Alto Software Into Perfect Malware

darkreading - 19 April 2024 04:20

It turns out that a powerful security solution can double as even more powerful malware, capable of granting comprehensive access over a targeted machine.

Cisco Warns of Massive Surge in Password-Spraying Attacks on VPNs

darkreading - 18 April 2024 21:39

Attackers are indiscriminately targeting VPNs from Cisco and several other vendors in what may be a reconnaissance effort, the vendor says.

CISA and Partners Release Advisory on Akira Ransomware

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.