Scottish Cyber Coordination Centre

Daily threat bulletin

29 April 2024

Vulnerabilities

Targeted operation against Ukraine exploited 7-year-old MS Office bug

Security Affairs - 28 April 2024 08:45

A hacking campaign targeted Ukraine exploiting a seven-year-old vulnerability in Microsoft Office to deliver Cobalt Strike. Security experts at Deep Instinct Threat Lab have uncovered a targeted campaign against Ukraine, exploiting a Microsoft Office vulnerability dating back almost seven years to deploy Cobalt Strike on compromised systems.

Over 1,400 CrushFTP internet-facing servers vulnerable to CVE-2024-4040 bug

Security Affairs - 26 April 2024 10:08

Over 1,400 CrushFTP internet-facing servers are vulnerable to attacks exploiting recently disclosed CVE-2024-4040 vulnerability. Over 1,400 CrushFTP internet-facing servers are vulnerable to attacks targeting the critical severity vulnerability CVE-2024-4040. CVE-2024-4040 is a CrushFTP VFS sandbox escape vulnerability. CrushFTP is a file transfer server software that enables secure and efficient file transfer capabilities.

Severe Flaws Disclosed in Brocade SANnav SAN Management Software

The Hacker News - 26 April 2024 20:33

Several security vulnerabilities disclosed in Brocade SANnav storage area network (SAN) management application could be exploited to compromise susceptible appliances.The 18 flaws impact all versions up to and including 2.3.0, according to independent security researcher Pierre Barre, who discovered and reported them.

Palo Alto Updates Remediation for Max-Critical Firewall Bug

darkreading - 26 April 2024 20:51

Though PAN originally described the attacks exploiting the vulnerability as being limited, they are increasingly growing in volume, with more exploits disclosed by outside parties.

Threat actors and malware

Okta warns of “unprecedented” credential stuffing attacks on customers

BleepingComputer - 27 April 2024 11:55

Okta warns of an “unprecedented” spike in credential stuffing attacks targeting its identity and access management solutions, with some customer accounts breached in the attacks. [...]

New ‘Brokewell’ Android Malware Spread Through Fake Browser Updates

Scottish Cyber Coordination Centre

The Hacker News - 26 April 2024 17:12

Fake browser updates are being used to push a previously undocumented Android malware called Brokewell. Brokewell is a typical modern banking malware equipped with both data-stealing and remote-control capabilities built into the malware," Dutch security firm ThreatFabric said in an analysis published Thursday.

Thousands of Qlik Sense Servers Open to Cactus Ransomware

darkreading - 26 April 2024 21:55

The business intelligence servers contain vulnerabilities that Qlik patched last year, but which Cactus actors have been exploiting since November. Swathes of organizations have not yet been patched.

Hackers Claim to Have Infiltrated Belarus' Main Security Service

SecurityWeek - 28 April 2024 16:46

A Belarusian hacker activist group claims to have infiltrated the network of the country's main KGB security agency and accessed personnel files of over 8,600 employees.

Self-Spreading PlugX USB Drive Malware Plagues Over 90k IP Addresses

SecurityWeek - 26 April 2024 14:41

More than 90,000 unique IPs are still infected with a PlugX worm variant that spreads via infected flash drives. The post Self-Spreading PlugX USB Drive Malware Plagues Over 90k IP Addresses appeared first on SecurityWeek.