Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

50th Release May 2023

China's Mustang Panda Hackers Exploit TP-Link Routers for Persistent Attacks

The Chinese nation-state actor known as Mustang Panda has been linked to a new set of sophisticated and targeted attacks aimed at European foreign affairs entities since January 2023.

An analysis of these intrusions, per Check Point researchers has revealed a custom firmware implant designed explicitly for TP-Link routers. “The implant features several malicious components, including a custom backdoor named 'Horse Shell' that enables the attackers to maintain persistent access, build anonymous infrastructure, and enable lateral movement into compromised networks," the company said.

Source:https://thehackernews.com/2023/05/chinas-mustang-panda-hackers-exploit-tp.html

Don't Click That ZIP File! Phishers Weaponizing .ZIP Domains to Trick Victims

A new phishing technique called "file archiver in the browser" can be leveraged to "emulate" a file archiver software in a web browser when a victim visits a .ZIP domain.

Threat actors, in a nutshell, could create a realistic-looking phishing landing page using HTML and CSS that mimics legitimate file archive software, and host it on a .zip domain, thus elevating social engineering campaigns. In a potential attack scenario, a miscreant could resort to such trickery to redirect users to a credential harvesting page when a file "contained" within the fake ZIP archive is clicked.

Source:https://thehackernews.com/2023/05/dont-click-that-zip-file-phishers.html

Barracuda Warns of Zero-Day Exploited to Breach Email Security Gateway Appliances

Email protection and network security services provider Barracuda is warning users about a zero-day flaw that it said has been exploited to breach the company's Email Security Gateway (ESG) appliances.

The zero-day is being tracked as CVE-2023-2868 and has been described as a remote code injection vulnerability affecting versions 5.1.3.001 through 9.2.0.006.

The California-headquartered firm said the issue is rooted in a component that screens the attachments of incoming emails.

Source:https://thehackernews.com/2023/05/barracuda-warns-of-zero-day-exploited.html

WebKit Under Attack: Apple Issues Emergency Patches for 3 New Zero-Day Vulnerabilities

Apple on Thursday rolled out security updates to iOS, iPadOS, macOS, tvOS, watchOS, and the Safari web browser to address dozens of flaws, including three new zero-days that it said are being actively exploited in the wild.

CVE-2023-32409 – to break out of the Web Content sandbox.

CVE-2023-28204 –issue in WebKit that could be abused to disclose sensitive information when processing web content.

Source:https://thehackernews.com/2023/05/webkit-under-attack-apple-issues.html

Critical Flaws in Cisco Small Business Switches Could Allow Remote Attacks

Cisco has released updates to address a set of nine security flaws in its Small Business Series Switches that could be exploited by an unauthenticated, remote attacker to run arbitrary code or cause a denial-of-service (DoS) condition.

"These vulnerabilities are due to improper validation of requests that are sent to the web interface," Cisco said, crediting an unnamed external researcher for reporting the issues. Four of the nine vulnerabilities are rated 9.8 out of 10 on the CVSS scoring system.

Source:https://thehackernews.com/2023/05/critical-flaws-in-cisco-small-business.html

New Flaw in WordPress Plugin Used by Over a Million Sites Under Active Exploitation

A security vulnerability has been disclosed in the popular WordPress plugin Essential Addons for Elementor that could be potentially exploited to achieve elevated privileges on affected sites.

"This plugin suffers from an unauthenticated privilege escalation vulnerability and allows any unauthenticated user to escalate their privilege to that of any user on the WordPress site," Patchstack researcher Rafie Muhammad said.

Successful exploitation of the flaw could permit a threat actor to reset the password of any arbitrary user as long as the malicious party is aware of their username. The shortcoming is believed to have existed since version 5.4.0.

This can have serious ramifications as the flaw could be weaponized to reset the password associated with an administrator account and seize full control of the website.

Source: https://thehackernews.com/2023/05/severe-security-flaw-exposes-over.html

New Ransomware Strain 'CACTUS' Exploits VPN Flaws to Infiltrate Networks

Cybersecurity researchers have shed light on a new ransomware strain called CACTUS that has been found to leverage known flaws in VPN appliances to obtain initial access to targeted networks.

Once inside the network, CACTUS actors attempt to enumerate local and network user accounts in addition to reachable endpoints before creating new user accounts and leveraging custom scripts to automate the deployment and detonation of the ransomware encryptor via scheduled tasks.

The ransomware has been observed targeting large commercial entities since March 2023, with attacks employing double extortion tactics to steal sensitive data prior to encryption. No data leak site has been identified to date.

Source:https://thehackernews.com/2023/05/new-ransomware-strain-cactus-exploits.html

Cloud Consultancy

Cloud Consultancy for Digitalization & Security – CCDS's is a Specialized Company in IT and Information Security Services, which has its international headquarters in the UAE. It also has branch offices throughout the MENA Region with its premier office in Saudi Arabia. Innovative and professional in its approach, it always partners with best-in-class products and services, to identify and solve security threats and issues for its clients.

Contact Us