Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

46th Release January 2023

Git Users Urged to Update Software to Prevent Remote Code Execution Attacks

The maintainers of the Git source code version control system have released updates to remediate two critical vulnerabilities that could be exploited by a malicious actor to achieve remote code execution.

The flaws, tracked as CVE-2022-23521 and CVE-2022-41903, impacts the following versions of Git: v2.30.6, v2.31.5, v2.32.4, v2.33.5, v2.34.5, v2.35.5, v2.36.3, v2.37.4, v2.38.2, and v2.39.0.

"The most severe issue discovered allows an attacker to trigger a heap-based memory corruption during clone or pull operations, which might result in code execution," the German cybersecurity company said of CVE-2022-23521.

Source:https://thehackernews.com/2023/01/git-users-urged-to-update-software-to.html

Cisco Issues Warning for Unpatched Vulnerabilities in EoL Business Routers

Cisco has warned of two security vulnerabilities affecting end-of-life (EoL) Small Business RV016, RV042, RV042G, and RV082 routers that it said will not be fixed, even as it acknowledged the public availability of proof-of-concept (PoC) exploit.

The issues are rooted in the router's web-based management interface, enabling a remote adversary to sidestep authentication or execute malicious commands on the underlying operating system.

The most severe of the two is CVE-2023-20025 (CVSS score: 9.0), which is the result of improper validation of user input within incoming HTTP packets.

Source:https://thehackernews.com/2023/01/cisco-issues-warning-for-unpatched.html

Twitter Denies Hacking Claims, Assures Leaked User Data Not from its System

Twitter on Wednesday said that its investigation found "no evidence" that users' data sold online was obtained by exploiting any security vulnerabilities in its systems.

"Based on information and intel analyzed to investigate the issue, there is no evidence that the data being sold online was obtained by exploiting a vulnerability of Twitter systems," the company said in a statement. "The data is likely a collection of data already publicly available online through different sources."

Source:https://thehackernews.com/2023/01/twitter-denies-hacking-claims-assures.html

Realtek Vulnerability Under Attack: Over 134 Million Attempts to Hack IoT Devices

Researchers are warning about a spike in exploitation attempts weaponizing a now-patched critical remote code execution flaw in Realtek Jungle SDK since the start of August 2022.

According to Palo Alto Networks Unit 42, the ongoing campaign is said to have recorded 134 million exploit attempts as of December 2022, with 97% of the attacks occurring in the past four months.

Source:https://thehackernews.com/2023/01/realtek-vulnerability-under-attack-134.html

Emotet Malware Makes a Comeback with New Evasion Techniques

The Emotet malware operation has continued to refine its tactics in an effort to fly under the radar, while also acting as a conduit for other dangerous malware such as Bumblebee and IcedID.

Emotet, which officially reemerged in late 2021 following a coordinated takedown of its infrastructure by authorities earlier that year, has continued to be a persistent threat that's distributed via phishing emails.

Source:https://thehackernews.com/2023/01/emotet-malware-makes-comeback-with-new.html

Microsoft Urges Customers to Secure On-Premises Exchange Servers

Microsoft is urging customers to keep their Exchange servers updated as well as take steps to bolster the environment, such as enabling Windows Extended Protection and configuring certificate-based signing of PowerShell serialization payloads.

"Attackers looking to exploit unpatched Exchange servers are not going to go away," the tech giant's Exchange Team said in a post. "There are too many aspects of unpatched on-premises Exchange environments that are valuable to bad actors looking to exfiltrate data or commit other malicious acts."

Exchange Server has been proven to be a lucrative attack vector in recent years, what with a number of security flaws in the software weaponized as zero-days to hack into systems.

Source: https://thehackernews.com/2023/01/microsoft-urges-customers-to-secure-on.html

Hive Ransomware Infrastructure Seized in Joint International Law Enforcement Effort

In what's a case of hacking the hackers, the darknet infrastructure associated with the Hive ransomware-as-a-service (RaaS) operation has been seized as part of a coordinated law enforcement effort involving 13 countries.

"Law enforcement identified the decryption keys and shared them with many of the victims, helping them regain access to their data without paying the cybercriminals," Europol said in a statement.

Hive, which sprang up in June 2021, has been a prolific cybercrime crew, launching attacks against 1,500 organizations in no less than 80 countries and netting it $100 million in illicit profits.

Source:https://thehackernews.com/2023/01/hive-ransomware-infrastructure-seized.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