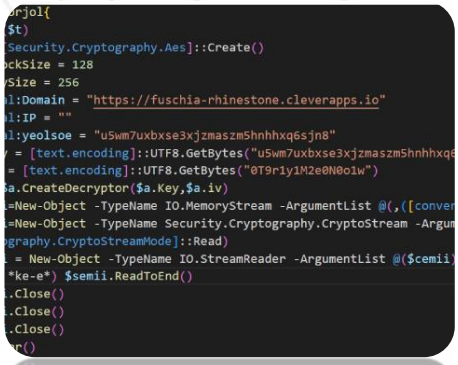
Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

51st Release June 2023



Iranian Hackers Using POWERSTAR Backdoor in Targeted Espionage Attacks

Charming Kitten, the nation-state actor affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC), has been attributed to a bespoke spear-phishing campaign that delivers an updated version of a fully-featured PowerShell backdoor called POWERSTAR.

"There have been improved operational security measures placed in the malware to make it more difficult to analyze and collect intelligence," Volexity researchers Ankur Saini and Charlie Gardner said in a report published this week.

Source:https://thehackernews.com/2023/06/iranian-hackers-charming-kitten-utilize.html

Zero-Day Alert: Apple Releases Patches for Actively Exploited Flaws in iOS, macOS, and Safari

Apple on Wednesday released a slew of updates for iOS, iPadOS, macOS, watchOS, and Safari browser to address a set of flaws it said were actively exploited in the wild.

The iPhone maker said it's aware that the two issues "may have been actively exploited against versions of iOS released before iOS 15.7," crediting Kaspersky researchers Georgy Kucherin, Leonid Bezvershenko, and Boris Larin for reporting them.

Apple has resolved a total of nine zero-day flaws in its products since the start of the year.

Source:https://thehackernews.com/2023/06/zero-day-alert-apple-releases-patches.html

Cybercriminals Hijacking Vulnerable SSH Servers in New Proxyjacking Campaign

An active financially motivated campaign is targeting vulnerable SSH servers to covertly ensnare them into a proxy network.

"This is an active campaign in which the attacker leverages SSH for remote access, running malicious scripts that stealthily enlist victim servers into a peer-to-peer (P2P) proxy network, such as Peer2Profit or Honeygain," Akamai researcher Allen West said in a Thursday report. "It is a stealthier alternative to cryptojacking and has serious implications that can increase the headaches that proxied Layer 7 attacks already serve," West said.

Source:https://thehackernews.com/2023/06/cybercriminals-hijacking-vulnerable-ssh.html

Newly Uncovered ThirdEye Windows-Based Malware Steals Sensitive Data

A previously undocumented Windows-based information stealer called ThirdEye has been discovered in the wild with capabilities to harvest sensitive data from infected hosts.

Fortinet FortiGuard Labs, which made the discovery, said it found the malware in an executable that masqueraded as a PDF file with a Russian name "СМК Правила оформления больничных листов.pdf.exe," which translates to "CMK Rules for issuing sick leaves.pdf.exe."
Source:https://thehackernews.com/2023/06/newly-uncovered-thirdeye-windows-based.html

New Fortinet's FortiNAC Vulnerability Exposes Networks to Code Execution Attacks

Fortinet has rolled out updates to address a critical security vulnerability impacting its FortiNAC network access control solution that could lead to the execution of arbitrary code.

Tracked as CVE-2023-33299, the flaw is rated 9.6 out of 10 for severity on the CVSS scoring system. It has been described as a case of Java untrusted object deserialization.

Source:https://thehackernews.com/2023/06/new-fortinets-fortinac-vulnerability.html

Experts Unveil Exploit for Recent Windows Vulnerability Under Active Exploitation

Details have emerged about a now-patched actively exploited security flaw in Microsoft Windows that could be abused by a threat actor to gain elevated privileges on affected systems.

The vulnerability, tracked as CVE-2023-29336, is rated 7.8 for severity and concerns an elevation of privilege bug in the Win32k component.

"An attacker who successfully exploited this vulnerability could gain SYSTEM privileges," Microsoft disclosed in an advisory issued last month as part of Patch Tuesday updates.

Win32k.sys is a kernel-mode driver and an integral part of the Windows architecture, being responsible for graphical device interface (GUI) and window management.

Source: https://thehackernews.com/2023/06/experts-unveil-poc-exploit-for-recent.html

Urgent Security Updates: Cisco and VMware Address Critical Vulnerabilities

VMware has released security updates to fix a trio of flaws in Aria Operations for Networks that could result in information disclosure and remote code execution.

The most critical of the three vulnerabilities is a command injection vulnerability tracked as CVE-2023-20887 (CVSS score: 9.8) that could allow a malicious actor with network access to achieve remote code execution.

Also patched by VMware is another deserialization vulnerability (CVE-2023-20888) that's rated 9.1 out of a maximum of 10 on the CVSS scoring system.

Source:https://thehackernews.com/2023/06/urgent-security-updates-cisco-and.html

Contact Us

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.