Cloud Consultancy

DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

58th Release - January 2024

Ivanti Discloses 2 New Zero-Day Flaws, One Under Active Exploitation

Ivanti is alerting of two new high-severity flaws in its Connect Secure and Policy Secure products, one of which is said to have come under targeted exploitation in the wild.

CVE-2024-21888 (CVSS score: 8.8) - A privilege escalation vulnerability in the web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.

CVE-2024-21893 (CVSS score: 8.2) - A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.
Sourcehttps://thehackernews.com/2024/01/alert-ivanti-discloses-2-new-zero-day.html

Outlook Vulnerability Could Leak Your NTLM Passwords

A now-patched security flaw in Microsoft Outlook could be exploited by threat actors to access NT LAN Manager (NTLM) v2 hashed passwords when opening a specially crafted file.

The issue, tracked as CVE-2023-35636 (CVSS score: 6.5), was addressed by the tech giant as part of its Patch Tuesday updates for December 2023.

In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file," Microsoft said in an advisory released last month. An attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability.
Source:https://thehackernews.com/2024/01/researchers-uncover-outlook.html

Citrix, VMware, and Atlassian Hit with Critical Flaws — Patch ASAP!

Citrix is warning of two zero-day security vulnerabilities in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) that are being actively exploited in the wild.

CVE-2023-6548 (CVSS score: 5.5) - Authenticated (low privileged) remote code execution on Management Interface (requires access to NSIP, CLIP, or SNIP with management interface access)

CVE-2023-6549 (CVSS score: 8.2) - Denial-of-service (requires that the appliance be configured as a Gateway or authorization and accounting, or AAA, virtual server).

Source:https://thehackernews.com/2024/01/citrix-vmware-anad-atlassian-hit-with.html

BY TOUSEEF UR REHMAN (CYBER SECURITY ANALYST – SOC TEAM)

Critical Cisco Flaw Lets Hackers Remotely Take Over Unified Comms Systems

Cisco has released patches to address a critical security flaw impacting Unified Communications and Contact Center Solutions products that could permit an unauthenticated, remote attacker to execute arbitrary code on an affected device.

Tracked as CVE-2024-20253 (CVSS score: 9.9), the issue stems from improper processing of user-provided data that a threat actor could abuse to send a specially crafted message to a listening port of a susceptible appliance.

Source:https://thehackernews.com/2024/01/critical-cisco-flaw-lets-hackers.html

Over 178,000 SonicWall Firewalls Potentially Vulnerable to Exploits

Over 178,000 SonicWall firewalls exposed over the internet are exploitable to at least one of the two security flaws that could be potentially exploited to cause a denial-of-service (DoS) condition and remote code execution (RCE).

"The two issues are fundamentally the same but exploitable at different HTTP URI paths due to reuse of a vulnerable code pattern," Jon Williams, a senior security engineer at Bishop Fox, said in a technical analysis shared with The Hacker News. CVE-2022-22274 & CVE-2023-0656

Source:https://thehackernews.com/2024/01/alert-over-178000-sonicwall-firewalls.html

Malware Using Google MultiLogin Exploit to Maintain Access Despite Password Reset

Information stealing malware are actively taking advantage of an undocumented Google OAuth endpoint named MultiLogin to hijack user sessions and allow continuous access to Google services even after a password reset.

According to CloudSEK, the critical exploit facilitates session persistence and cookie generation, enabling threat actors to maintain access to a valid session in an unauthorized manner.

The company recommended users turn on Enhanced Safe Browsing in Chrome to protect against phishing and malware downloads.

"It's advised to change passwords so the threat actors wouldn't utilize password reset auth flows to restore passwords," Karthick said. "Also, users should be advised to monitor their account activity for suspicious sessions which are from IPs and locations which they don't recognize."

Source: https://thehackernews.com/2024/01/malware-using-google-multilogin-exploit.html

Opera MyFlaw Bug Could Let Hackers Run ANY File on Your Mac or Windows

Cybersecurity researchers have disclosed a now-patched security flaw in the Opera web browser for Microsoft Windows and Apple macOS that could be exploited to execute any file on the underlying operating system.

The remote code execution vulnerability has been codenamed MyFlaw by the Guardio Labs research team owing to the fact that it takes advantage of a feature called My Flow that makes it possible to sync messages and files between mobile and desktop devices.

"This is achieved through a controlled browser extension, effectively bypassing the browser's sandbox and the entire browser process," the company said in a statement shared with The Hacker News.

Source:https://thehackernews.com/2024/01/opera-myflaw-bug-could-let-hackers-run.html

Contact Us

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.