QUALYSEC
BEYOND CYBERSECURITY

2023
OCT 1ST WEEK
CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

Cisco Emergency Responder Vulnerability Let Remote Attacker Login as Root User

Cisco was reported with a critical vulnerability that could allow threat actors to log in to the affected devices as a root account. The CVE for this vulnerability has been given as CVE-2023-20101 and has a severity of 9.8 (Critical).

Cisco has released a security advisory for addressing this vulnerability, and patches have been updated for the affected products.

CVE-2023-20101: Cisco Emergency Responder Static Credentials Vulnerability

This particular vulnerability exists due to static user credentials for the root account configured during development. The root account has default and static credentials that cannot be changed or deleted.

If a threat actor successfully exploits, it could allow them to log in to the affected system and execute arbitrary commands as the root user. There are no workarounds for this vulnerability. However, there is no evidence that this vulnerability is being exploited in the wild.

Cisco has recommended that users of this product upgrade to the latest version of Cisco Emergency Responder to prevent this vulnerability from getting exploited.

Source : https://cybersecuritynews.com/cisco-emergency-responder-vulnerability/

ZenRAT Malware Delivered Through Fake Bitwarden Installation Packages

According to the recent findings by Proofpoint, a new malware called ZenRAT has been discovered. This malware is being spread via fraudulent download packages disguised as Bitwarden installations.

This malware primarily targets Windows users and redirects non-Windows users to benign web pages.

The method of distribution remains unknown, but historical precedents include SEO Poisoning, adware bundles, and email.

ZenRAT is a modular Remote Access Trojan (RAT) with information-stealing capabilities.

The threat landscape in the digital realm is ever-evolving, with malicious actors constantly devising new tactics to exploit unsuspecting victims.

On August 10, 2023, Jérôme Segura, Senior Director of Threat Intelligence at Malwarebytes, brought to light a concerning discovery – a malware sample concealed within a Windows software installation package.

This sample was initially found on a website posing as Bitwarden, bitwariden[.]com, an eerily convincing replica of the legitimate Bitwarden website, reads the report.

Source : https://cybersecuritynews.com/zenrat-malware-bitwarden/

Zero-Day WhatsApp Hacking Vulnerabilities Worth Millions

Securing the devices running iOS and Android operating systems is now costly due to improved defenses.

According to a recent report by TechCrunch, there has been a surge in the demand for zero-day exploits that can be used to hack into popular instant messaging apps like WhatsApp.

These exploits are now being sold for millions of dollars, highlighting the growing threat of cyber attacks on communication platforms that are widely used by millions of people across the globe.

It is important for users to be vigilant and take necessary precautions to secure their personal and sensitive information while using these apps.

Recently, a Russian firm sought to purchase undisclosed software vulnerabilities for $20 million, exclusively for Russian government and private sector use, enabling remote access to iOS and Android phones.

The high price reflects limited researchers willing to cooperate due to the Ukraine situation, with Russian government customers willing to pay extra.

Zero-Days Worth Millions of Dollars

Beyond Russia, even in niche app markets, zero-day prices have surged significantly as the leaked documents reveal that in 2021, a WhatsApp Android bug enabling message access ranged from $1.7 to $8 million.

Source : https://cybersecuritynews.com/zero-days-for-hacking-whatsapp/

Supershell – Open-Source Botnet That Obtain SSH Shell Access

The digital age offers opportunities but also increases the importance of cybersecurity as threats grow in complexity and sophistication, making preparedness a top priority.

Open-source botnets are now a hot topic in cybersecurity due to their accessibility and rapid adaptability against security measures.

Cybersecurity researchers at SOCRadar recently reported about an open-source botnet, Supershell, that obtains SSH shell access.

Supershell Botnet

Supershell is an open-source botnet that offers rapid one-click Docker-based deployment with integrated reverse SSH for team collaboration and interactive control.

This botnet deploys small client payloads across multiple platforms, enabling SSH server setup for rapid access and offering a versatile range of functions.

Researchers closely analyzed recently discovered Supershell Botnet Panels, taking an operational approach to gain deeper insights through panel infiltration.

Security analysts successfully tracked active Supershell panels using a tailored Urlscan search query, revealing valuable insights.

Source : https://cybersecuritynews.com/supershell-open-source-botnet/

Threat Actors Deployed Hundreds of Python Packages to Steal System Data

In the open-source ecosystem, shadows shift as collaboration succeeds, attracting both novices and skilled threat actors. A rising threat has been evolving and sharpening its tools in recent months.

Checkmarx Supply Chain Security researchers have tracked a malicious actor since April, documenting their evolving tactics as they refine their skills.

Beginning in April 2023, an unidentified attacker pounded the Python environment with dozens of closely related malicious packages, generating 75,000 downloads and raising suspicions about a hidden objective

The attacker's initial packages appeared innocent, written in plain text, gradually infiltrating systems for their nefarious purposes.

Malicious Python Packages

Dependencies are installed silently, with the attacker employing subprocessing to avoid detection. The malware behaved like a vigilant predator, evading any signs of danger.

.

Source : https://cybersecuritynews.com/malicious-python-packages/

Apple Emergency Update for New Zero-Day Used to Hack iPhones

Apple has discovered a Zero-day vulnerability affecting iOS and iPadOS versions earlier than 17.0.3, which could allow threat actors to elevate their privileges. The CVE for this vulnerability has been given as CVE-2023-42824, and the severity of this vulnerability is currently being analyzed.

It was also mentioned that iOS 16.6 versions are actively being targeted with this vulnerability by threat actors for exploitation.

Apple has addressed this new Zero-day along with CVE-2023-5217 that affected libvpx, a Heap buffer overflow in vp8 encoding. Moreover, several Chromium-based browsers have used this particular vulnerability, including Microsoft Edge, Google Chrome, and Mozilla Firefox.

All the affected vendors have published their security advisories for addressing this vulnerability. This vulnerability has a severity of 8.8 (High) given by the National Vulnerability Database (NVD).

CVE-2023-42824 – Privilege Escalation

Apple states that threat actors exploit this vulnerability to elevate their privileges. There has been no evidence of a publicly available exploit for this vulnerability.

Source : https://cybersecuritynews.com/apple-emergency-zero-day-update/

Sony Breached Via MOVEit Zero-Day Vulnerability

Sony Interactive Entertainment (SIE) discloses a cybersecurity breach caused by the exploitation of a zero-day vulnerability in Progress Software's MOVEit Transfer platform.

Nearly 6791 current and former workers or members of their families who reside in the United States were impacted by the data breach, which includes some personal information.

The ClOp ransomware group, a criminal organization with ties to Russia, claimed responsibility for carrying out the attack. The group allegedly took data from Sony in June.

Insights of the Sony's Cybersecurity Breach

According to the Data breach notice, Progress Software, which is utilized by SIE and countless other businesses worldwide, disclosed a newly identified vulnerability in its MOVEit file transfer platform on May 31, 2023. Before Progress Software disclosed the flaw, the company said they were made aware of it on May 28, 2023; an unauthorized actor used the flaw to obtain certain SIE files kept on its MOVEit platform.

The company found the unauthorized downloads on June 2, 2023, promptly took the platform offline, and fixed the issue. After that, an inquiry was started with support from outside cybersecurity professionals. Law enforcement was also informed.

Source : https://cybersecuritynews.com/sony-breached-moveit-zero-day/

Malicious npm Package from a Twin Developers Deliver r77 Rootkit

A malicious supply chain attack affecting the popular npm platform, often used for Node.js projects, has been identified.

This attack employs a tactic known as typosquatting, where malicious actors create packages with names strikingly similar to legitimate ones to deceive developers.

Cybersecurity researchers at ReversingLabs have unveiled a concerning trend in the realm of open-source software development.

In this case, a seemingly harmless typo of a single letter “s” differentiates a legitimate npm package from its malicious twin, leading to the delivery of the r77 rootkit, a dangerous form of malware.

Typosquatting Campaign’s Deceptive Package

The malicious npm package at the center of this campaign goes by the name “node-hide-console-windows.”

It cunningly mimics the legitimate npm package “node-hide-console-window,” which is utilized for toggling an application’s console window visibility. The similarity between the two names is so subtle that it easily escapes notice. This malicious package was discovered to have been downloaded over 700 times before it was detected and removed by npm maintainers.

Source : https://cybersecuritynews.com/malicious-npm-package-deliver-r77-rootkit/

Exim SMTP Service Zero-day Flaw Let Attackers Execute Remote Code

Six new zero-day vulnerabilities in Exim Message Transfer Agent have been reported as part of the Zero-Day initiative. These vulnerabilities were discovered in June 2022 but were not disclosed until now as Exim did not fix them.

Though these vulnerabilities have been published now, only three of the six vulnerabilities were fixed, which include 1 Critical severity (9.8), 1 high severity (8.1), and 1 low severity (3.7) vulnerabilities.

Fixed Vulnerabilities

The vulnerability that had the highest severity among the six reported vulnerabilities was CVE-2023-42115 associated with an out-of-bounds write in Exim AUTH, resulting in remote code execution. This vulnerability had the highest severity of 9.8 (Critical), which Exim fixed.The high vulnerability fixed by Exim was CVE-2023-42116, which was related to a stack-based buffer overflow that exists due to improper validation in the handling of NTLM challenge requests, resulting in remote code execution. This vulnerability has a severity of 8.1 (High). In addition to this, the other low-severity vulnerability was CVE-2023-42114, which was linked with an out-of-bounds read leading to information disclosure. The severity of this vulnerability was 3.7 (Low), which Exim also fixed.

Source : https://cybersecuritynews.com/exim-smtp-zero-day/

French Cybercriminal Pleads Guilty for Hacking Corporate Data

In a significant development in the realm of cybercrime, a 22-year-old French citizen, Sebastien Raoult, also known as Sezyo Kaizen, has pleaded guilty to conspiracy to commit wire fraud and aggravated identity theft in the U.S. District Court in Seattle.

This case sheds light on a sophisticated cybercriminal operation that utilized phishing emails and deceptive tactics to breach corporate systems, resulting in a total loss estimated to exceed $6 million for victim companies.

The Arrest and Extradition:

Sebastien Raoult's journey through the legal system began with his arrest in Morocco last year.

Following his apprehension, he was subsequently sent back to the United States in January 2023 to face charges related to cybercrimes committed alongside two co-conspirators.

The accusation, handed down by a grand jury in the Western District of Washington in June 2021, marked the start of legal proceedings against the cybercriminal trio.

Source : https://cybersecuritynews.com/french-cybercriminal-pleads-guilty/

New Android Banking Malware Pose as Government App to Target Users

Cybercriminals continue making malware for profit, with a recent report uncovering ASMCrypt in underground forums related to the DoubleFinger loader.

In the cybercrime landscape, researchers at Securelist have also reported on new Lumma stealer and Zanubis Android banking malware versions.

Researchers discovered an ad for ASMCrypt, a cryptor/loader variant designed to avoid AV/EDR detection, resembling the DoubleFinger loader.However, researchers strongly suspect ASMCrypt is an evolved DoubleFinger version, acting as a 'front' for a TOR network service, though with some differences in operation.

New Android Banking Malware

Buyers get the ASMCrypt binary, which connects to the malware's TOR backend using hardcoded credentials and then displays the options menu. Once options are chosen and the build button pressed, the app conceals an encrypted blob in a .png file to be uploaded on an image hosting site. Simultaneously, the cybercriminals create and distribute the malicious DLL or binary, reads the report.

Source :https://cybersecuritynews.com/new-android-banking-malware-government-app/

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT