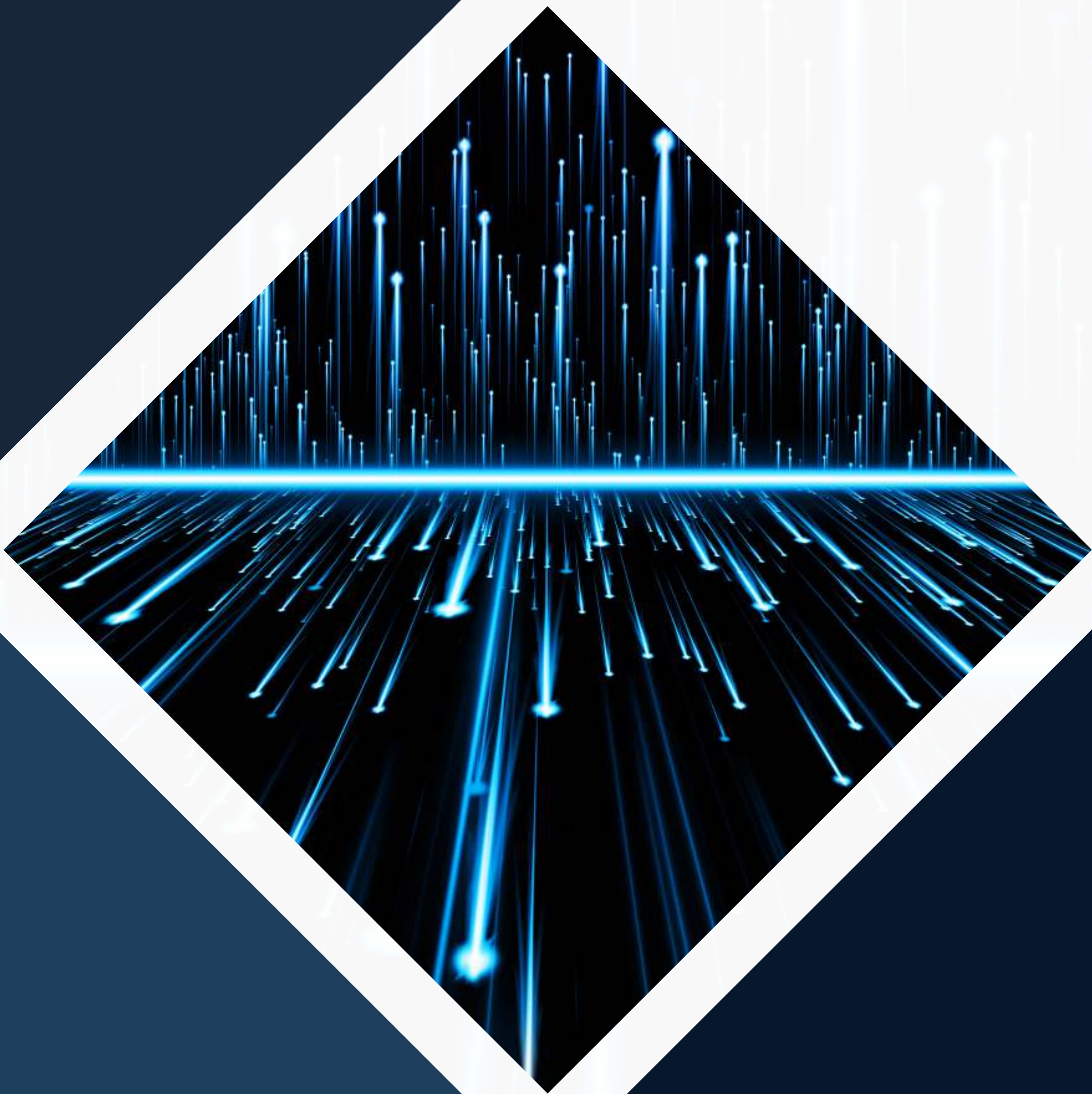
SCC



JANUARY

THREAT PULSE

IN THE NEWS THIS MONTH

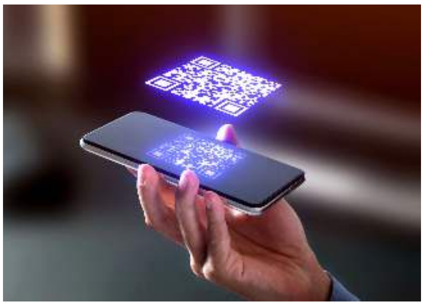
11 Million SSH Servers at Risk of Latest Terrapin Attacks

Over 11 million Internet-exposed SSH servers may be at risk of the Terrapin attack which can compromise the integrity of some SSH connections. This attack alters sequence numbers during the handshake process, especially when certain encryption modes are utilized like ChaCha20-Poly1305 or CBC with Encrypt-then-MAC.

READ MORE

Theft via QR Code Phishing Rises by 587%: Social Engineering Scams on the Rise

QR-code-based phishing attacks increased by 587%, due to the lack of QR code protection in email security solutions and the widespread use of scanning QR codes. Security vendors developed new protections, but threat actors responded with a new variation of attacks. There has also been an increase in YouTube stream-jacking campaigns for cryptocurrency theft using deepfake videos.



READ MORE

More Than 150k WordPress Websites at Risk of Takeover Due to Vulnerable Plugin

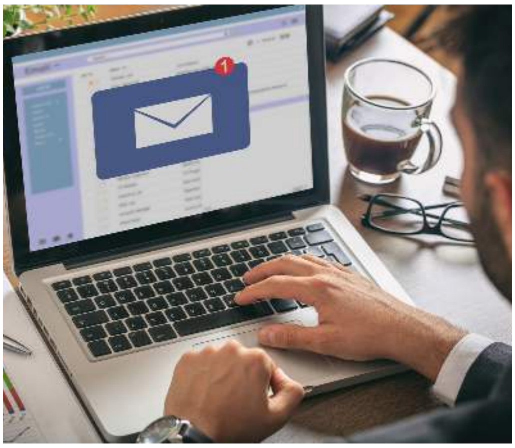
The POST SMTP Mailer WordPress plugin used by 300,000 websites has two vulnerabilities that could allow an attacker to reset the API key and view sensitive information, including password reset emails.

The attacker can use a function related to the mobile app to set a valid token for the authentication key via a request, potentially taking control of the site authentication without verification.

READ MORE

TOP OF THE NEWS THIS MONTH

SMTP Smuggling: New Flaw Lets Attackers Bypass Security and Spoof Emails

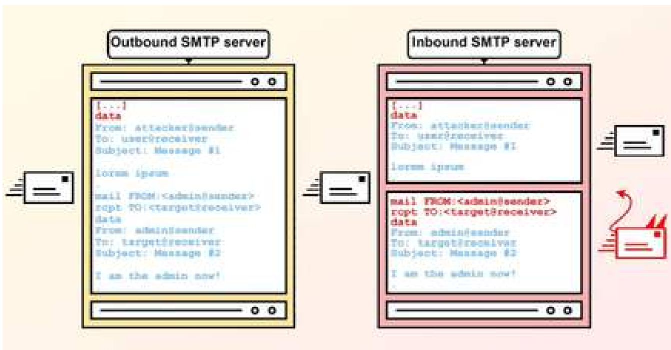


Threat actors could abuse vulnerable SMTP servers worldwide to send malicious emails from arbitrary email addresses using a newly discovered exploitation technique of the Simple Mail Transfer Protocol called, SMTP smuggling.

This can be weaponized by threat actors to send spoofed emails with fake sender addresses while bypassing security measures.

SMTP smuggling exploits security vulnerabilities in Cisco, Microsoft, GMX, Postfix, and Sendmail servers to spoof millions of domains. SMTP is a TCP/IP protocol used to send and receive email messages over a network. To relay a message from an email client (aka mail user agent), an SMTP connection is established between the client and server in order to transmit the actual content of the email.

In SMTP smuggling, attackers exploit how inbound and outbound SMTP servers interpret the end-of-data code sequence used in messaging — "<CR> <LF>.<CR> <LF>" — to give SMTP a different understanding of where the message data ends, allowing an attacker to break out of the message data, specify arbitrary SMTP commands, and/or even send separate emails.



READ MORE

TOP OF THE NEWS THIS MONTH

CISA Flags Active Exploitation of Microsoft SharePoint Vulnerability

CISA has advised of a critical security vulnerability impacting Microsoft SharePoint Server and has added this to its Known Exploited Vulnerabilities as it has been seen actively exploited in the wild.

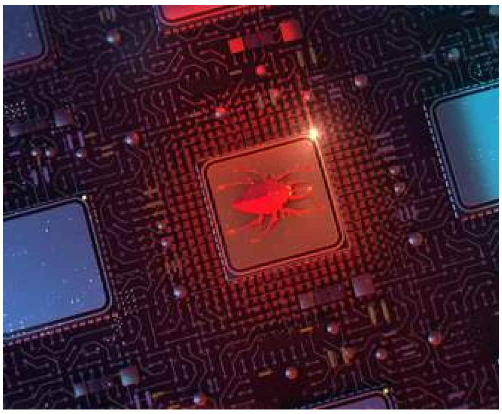
The issue, tracked as CVE-2023-29357 (CVSS score: 9.8), is a privilege escalation flaw that could be exploited by an attacker to gain administrator privileges.

The issue, tracked as CVE-2023-29357 (CVSS score: 9.8), is a privilege escalation flaw that could be exploited by an attacker to gain administrator privileges. An attacker who has gained access to spoofed JWT authentication tokens can use them to execute a network attack which bypasses authentication and allows them to gain access to the privileges of an authenticated user.

READ MORE

Feds Warn of AndroxGh0st Botnet Targeting AWS, Azure, and Office 365 Credentials

AndroxGh0st is a Python-based malware that targets servers with known security flaws to access Laravel environment files and steal credentials for high-profile applications such as AWS and Microsoft Office 365.



It has inspired the creation of similar tools like AlienFox, GreenBot (Maintance), Legion, and Predator. Its discovery was made by Lacework in December 2022.

Some of the notable flaws weaponized by the attackers include CVE-2017-9841(PHPUnit), CVE-2021-41773 (Apache HTTP Server), and CVE-2018-15133 (Laravel Framework).

READ MORE

SCC

VULNERABILITIES AND EXPLOITS

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

Notable Vulnerabilities and exploits for this month:

CVE-2024-20253

Cisco Unified Communications Products Remote Code Execution Vulnerability

CVSS SCORE 9.9

CVE-2024-23224

Apple Mac OS Ventura / Sonoma arbitrary code with kernel privileges Vulneribilty

CVSS SCORE 9.1

CVE-2024-21887

Ivanti Connect Secure Command Injection Vulnerability

CVSS SCORE 9.1

CVE-2023-29298, CVE-2023-38203

Adobe ColdFusion Code Execution vulnerabilities

CVSS SCORE 9.8

CVE-2023-39336

Ivanti Endpoint Manager (EPM) solution Remote Code Execution (RCE) Vulnerability

CVSS SCORE 9.6

PHISHING NEWS

Alert: Invoice Phishing Scam Featuring TA866 and Malware Seeds

TA866, a threat actor known for delivering malware families such as WasabiSeed and Screenshotter, has launched a new large-scale phishing campaign after a nine-month hiatus.

The campaign involved sending invoice-themed emails with decoy PDF files containing OneDrive URLs that led to a multi-step infection chain and eventually delivered the malware payload.

READ MORE

New Year, New Scams – Health product scam campaigns abusing cheap Top Level-Demands

There is a rise in health product scams that use cheap top-level domains and impersonate reputable organizations like Fox News, the Daily Mail, The Today Show, and the New York Times. These campaigns use affiliate links to direct users to landing pages that sell products, and they are often promoted on social media platforms like Facebook, where compromised accounts are used to advertise scams through phishing websites.

READ MORE

There is a Ransomware Armageddon Coming for Us All

A CISA and Cisco report reveals that 90% of data breaches occur due to phishing attacks, resulting in monetary losses exceeding $10 billion.

Generative AI can facilitate sophisticated phishing attacks, which only wearable FIDO2-compliant devices can prevent. The next-generation MFA paradigm relies on such devices, which eliminate the human factor in phishing.

READ MORE

Patch Tuesday - January Updates

Microsoft updates:

Microsoft Addresses 49 Vulnerabilities in January's 2024 Patch Tuesday Microsoft has identified and addressed 49 vulnerabilities, including one critical remote code execution vulnerability, in January's 2024 Patch Tuesday. Note that four browser vulnerabilities were published separately this month and are not included in the total. No zero-day vulnerabilities have been published for this month..

Critical and Important Vulnerabilities:

CVE-2024-0057- NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability 9.1 (Important)

A security feature bypass vulnerability exists when Microsoft .NET Framework-based applications use X.509 chain building APIs. An attacker could present an arbitrary untrusted certificate with malformed signatures, triggering a bug in the framework. The bug consists of the APIs not completely validating the X.509 certificate due to a logic flaw, as a result an incorrect reason code would be returned which some applications may utilize to trust and may inadvertently treat this scenario as a successful chain build.

CVE-2024-20674 - Windows Kerberos Security Feature Bypass Vulnerability - 9.0 (Critical)

A flaw in the Windows implementation of Kerberos. By establishing a machine-in-the-middle (MitM), an attacker could trick a client into thinking it is communicating directly with the Kerberos authentication server, and subsequently bypass authentication and impersonate the client user on the network. An however must first gain access to the restricted network before running an attack. This relationship can then be leveraged to intercept valid Kerberos authentication sessions and enable the attacker to harvest credentials. All current versions of Windows receive a patch.

A full list of Vulnerabilities disclosed by Microsoft can be found here

Patch Tuesday - January Updates

Fortinet updates:

CVE-2023-44250 - FortiOS & FortiProxy - Improper authorization for HA requests - CVSS 8.3 (High)

An improper privilege management vulnerability in a FortiOS & FortiProxy HA cluster may allow an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.

READ MORE

ZOOM updates:

CVE-2023-49647 - Zoom VDI Client for Windows and Zoom SDKs for Windows- Improper Access Control – 8.8 (High)

Improper access control in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows before version 5.16.10 may allow an authenticated user to conduct an escalation of privilege via local access.

READ MORE

Other vendors who released updates for December:

Cisco - released security updates for a privilege elevation flaw in the Cisco Identity Services Engine.

Google - released the Android January 2024 security updates.

Ivanti - released security updates for a critical remote code execution (RCE) vulnerability in its Endpoint Management software (EPM)

KyberSlash - a new Kyberslash attack puts numerous Quantum encryption projects at risk.

SAP - has released its January 2024 Patch Day updates.

Adobe - released a single patch addressing six CVEs in Substance 3D Stager . All six bugs are rated Important with the most severe allowing arbitrary code execution.