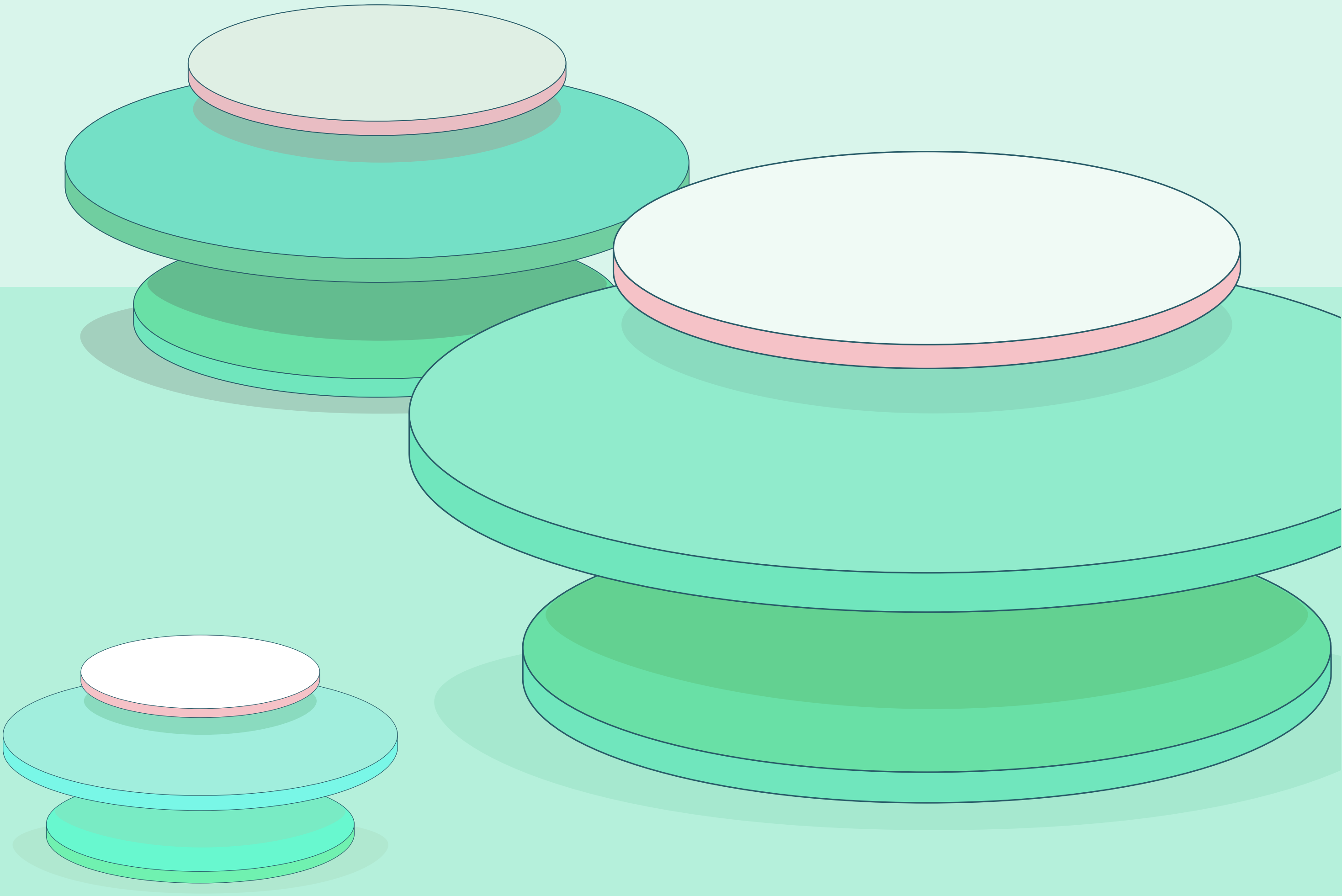
VULCAN.



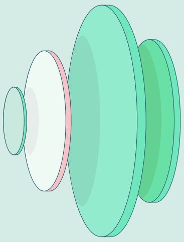
Q3 2024

Vulnerability Watch

Quarterly trends, themes and insights from
the world of cyber security vulnerabilities

Table of contents

Introduction



This report highlights significant vulnerabilities identified in the third quarter of 2024. Updated through September 27th, it describes the possible repercussions of these vulnerabilities and provides suggestions for organizations to bolster their exposure management practices. As with previous iterations, while the report offers detailed technical information on CVEs, it also delves deeper than just the Common Vulnerability Scoring System (CVSS) severity rating by incorporating data about their Exploitability Score (EPSS) and their listing in the Cybersecurity and Infrastructure Security Agency (CISA) catalog, along with other pertinent information.

The story of Q3 2024

Q3 2024 has been a challenging quarter. With a surge in state-sponsored cyber attacks (as we'll explore below) and a continued rise in vulnerabilities, organizations are grappling with serious concerns about their exposure risk management. As compliance regulations become more stringent and cyber criminals more audacious, security teams are encountering some of their most daunting challenges to date.

Here are some of the key stories:

Iran-based ransomware threats

The recent advisory from the FBI, CISA, and DC3 highlights a significant escalation in ransomware attacks from Iran-based threat actors. By targeting vulnerabilities in critical network devices like Citrix Netscaler and Checkpoint Security Gateway, these cyber actors are exploiting weaknesses in U.S. organizations' defenses.

This growing threat underlines the importance of robust cyber security practices, as attacks can cause significant financial and operational damage. The advisory stresses the need for proactive measures like regular patching and multi-factor authentication, emphasizing how crucial it is for organizations to stay ahead of these evolving threats.

PHP and application flaws

In Q3 2024, vulnerabilities in PHP installations have increased, leading to privilege escalation, remote code execution, and malware attacks like trojans, miners, and ransomware. Experts recommend updating PHP, strengthening security, and monitoring for compromise, emphasizing proactive cyber security.

Critical infrastructure attacks

The Cybersecurity and Infrastructure Security Agency (CISA) have dominated cyber security news with warnings and reports about attacks on critical infrastructure. They also released #StopRansomware[1] advisories for Black Basta[2] and Akira ransomware, attributing the initial access in these cases to exploited application vulnerabilities.

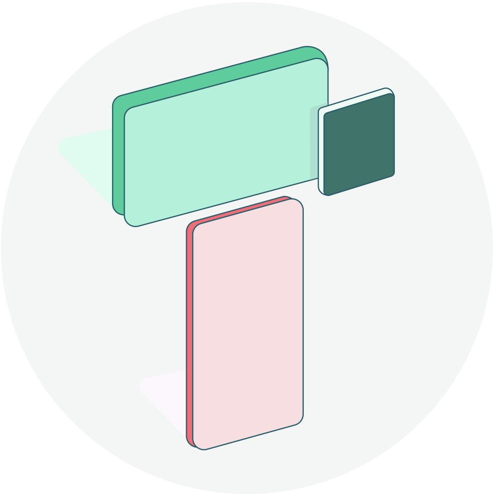
According to CISA's Known Exploited Vulnerabilities (KEV) list, 39% of attacks[3] were linked to application flaws, pointing to a growing risk for unpatched, internet-exposed systems. Initial access in data breaches and ransomware incidents was primarily achieved through info-stealer and loader malware, with SocGholish[4] and Atomic Stealer[5] being particularly active.

Breaches involving customers of the Snowflake data platform persisted, especially among organizations that hadn't enforced multi-factor authentication (MFA) on their accounts. While only approximately 7% of the impacted organizations have officially confirmed a breach as of June 2024, more disclosures are anticipated as companies approach regulatory deadlines for breach notification.

Additionally, during the last quarter, more than 55 million individuals were affected by data breaches unrelated to Snowflake, compromising sensitive data such as payment information, login credentials, and healthcare records.

SQL injection

In Q3 2024, SQL injection attacks remained a top threat to PHP and ASP applications, with automated tools increasingly used to exploit vulnerabilities in MySQL, Microsoft SQL Server, and PostgreSQL.
Despite being well-known, these attacks persist, especially in legacy systems. Experts urged using prepared statements, input validation, and bot management to mitigate risks, emphasizing the need for ongoing developer education and security training.



[1] Stop Ransomware | CISA
[2] CISA and Partners Release Advisory on Black Basta Ransomware
[3] Q3 Threat Intelligence Report: Trending Malware, Breaches, and Vulnerabilities | Ericsson
[4] SocGholish, Software S1124 | MITRE ATT&CK®
[5] Rise of Atomic Stealer signals a sea change in macOS malware - ThreatDown by Malwarebytes

Notable vulnerabilites of Q3 2024

CVE-2024-6409

Affected products:	OpenSSH
Product category:	Networking
Severity:	CVSS (Red Hat): 7 | EPSS: 0.044%
Type:	Signal handler race condition
Impact:	Remote code execution as an unprivileged user
PoC:	No
Exploit in the wild:	No confirmed evidence
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

Following late June's RegreSSHion vulnerability, CVE-2024-6409 is a critical race condition vulnerability in OpenSSH's server component (sshd) affecting versions 8.5p1 to 9.8p1 on glibc-based Linux systems. It could potentially allow remote code execution as an unprivileged user. The vulnerability arises from unsafe signal handling when authentication times out. It's recommended to upgrade to OpenSSH 9.4 or later to mitigate this issue.

CVE-2024-38856

Affected products:	Apache OFBiz versions up to 18.12.14
Product category:	Enterprise Resource Planning (ERP) Software
Severity:	CVSS: 9.8 | EPSS: 93.274%
Type:	Remote code execution
Impact:	Confidentiality, integrity, availability
PoC:	Link
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-38856 is a critical security vulnerability in Apache OFBiz versions up to 18.12.14. It allows unauthenticated remote code execution due to incorrect authorization. The vulnerability has a high severity rating (CVSSv3.1 Base Score: 8.1) and affects how OFBiz processes request parts differently for authentication and page rendering. Users should upgrade to version 18.12.15 or later to mitigate this risk.

0.0.0.0 day browser vulnerability

Affected products:	Major web browsers including Chrome, Firefox, and Safari on macOS and Linux systems
Product category:	Web browser
Severity:	High
Type:	Unauthorized access (via allowing malicious sites to interact with local services)
Impact:	Possibly Remote Code Execution
PoC:	Link
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	N/A

The 0.0.0.0 Day vulnerability is a critical security flaw affecting major web browsers on macOS and Linux. It allows malicious websites to bypass browser security and access local network services by exploiting how browsers handle the IP address 0.0.0.0. This 18-year-old vulnerability can lead to unauthorized access and remote code execution. Browser vendors are working on fixes, with Chrome, Safari, and Firefox planning to block access to 0.0.0.0. Users should keep browsers updated and implement additional security measures to protect local services.

CVE-2024-7589

Affected products:	All supported versions of FreeBSD with OpenSSH enabled
Product category:	Operating system
Severity:	CVSS: 8.1 | EPSS: 0.063%
Type:	Signal Handler Race Condition
Impact:	Remote code execution (RCE)
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-7589 is a critical race condition vulnerability in OpenSSH on FreeBSD. It allows remote attackers to potentially execute arbitrary code with root privileges. The flaw affects all supported FreeBSD versions with OpenSSH enabled. FreeBSD has released emergency patches for affected versions. Users are strongly advised to update their systems immediately or set LoginGraceTime to 0 in sshd_config as a temporary workaround. The vulnerability has a high severity rating due to its potential for full system compromise.

CVE-2024-38206

Affected products:	Microsoft Copilot
Product category:	AI/LLM
Severity:	CVSS (Microsoft): 8.5 | EPSS: 0.063%
Type:	Bypass Server-Side Request Forgery (SSRF)
Impact:	Information disclosure
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-38206 is a Server-Side Request Forgery (SSRF) vulnerability in Microsoft Copilot Studio. It allows authenticated attackers to bypass SSRF protection, potentially leaking sensitive network information. Microsoft has already mitigated the issue and states no action is required from users. There's no evidence of active exploitation, and the company released this information for transparency.

CVE-2024-37085

Affected products:	VMware ESXi 8.0 | VMware ESXi 7.0
Product category:	Third-party software
Severity:	CVSS: 7.2 | EPSS: 1.412%
Type:	Authentication bypass
Impact:	Gain full access to an ESXi host
PoC:	Link
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-37085 is a critical authentication bypass vulnerability in VMware ESXi hypervisors' Active Directory integration. It allows attackers to gain full administrative privileges on domain-joined ESXi systems by exploiting a flaw in the "ESX Admins" group verification. Multiple ransomware groups are actively exploiting this vulnerability. Affected versions include ESXi 8.0 and 7.0, and some Cloud Foundation versions.

CVE-2024-7593

Affected products:	Ivanti Virtual Traffic Manager versions 22.2 – 22.7R1
Product category:	Application delivery controller
Severity:	CVSS: 9.8 | EPSS: 93.709%
Type:	Authentication bypass of admin panel
Impact:	Potentially complete system compromise
PoC:	Link
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2024-7593 is a critical authentication bypass vulnerability in Ivanti Virtual Traffic Manager (vTM). It allows unauthenticated attackers to create administrator accounts on affected systems. The flaw has a CVSS v3.1 score of 9.8 (Critical) and affects versions other than 22.2R1 and 22.7R2. Exploit code is publicly available. Ivanti strongly recommends immediate upgrading to patched versions. Temporary mitigations include restricting admin access or limiting access to trusted IP addresses. Over 400 potentially vulnerable internet-facing instances have been identified.

CVE-2024-4879

Affected products:	ServiceNow Vancouver | Washington DC Now | Utah platform releases
Product category:	IT service management
Severity:	CVSS: 9.8 | EPSS: 96.507%
Type:	Input validation
Impact:	Remote code execution
PoC:	Link
Exploit in the wild:	No
CISA catalog:	Yes
Remediation action:	Update version
MITRE advisory:	Read more

CVE-2024-4879 is a critical vulnerability in ServiceNow's Vancouver and Washington DC versions, discovered in 2024. It's a Jelly Template Injection flaw that allows unauthenticated remote code execution, potentially leading to severe data breaches and system compromises. With a CVSSv4.0 Base Score of 9.8, it poses a significant threat, especially when chained with other vulnerabilities. Active exploitation attempts have been observed across various industries, particularly in financial services. ServiceNow released security updates on July 10, 2024, and organizations are strongly advised to apply these patches immediately to mitigate the risk.

CVE-2024-23663

Affected products:	FortiExtender 7.4 - 7.4.0 through 7.4.2 FortiExtender 7.2 - 7.2.0 through 7.2.4 FortiExtender 7.0 - 7.0.0 through 7.0.4
Product category:	Networking
Severity:	CVSS: 8.8 | EPSS: 0.05%
Type:	Improper access control
Impact:	Privilege Escalation
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Apply patches
MITRE advisory:	Read more

CVE-2024-23663 is a critical vulnerability affecting the Linux kernel's netfilter subsystem. It allows a local attacker with unprivileged user access to escalate privileges to root, potentially leading to full system compromise. The flaw stems from a use-after-free bug in the nf_tables networking framework. Discovered in early 2024, it affects Linux kernel versions 5.10 through 6.1. The vulnerability has a CVSS v3.1 base score of 8.8, indicating high severity. Linux distributions have released patches to address this issue, and users are strongly advised to update their systems promptly to mitigate the risk of exploitation.

CVE-2024-29847

Affected products:	Ivanti EPM
Product category:	Endpoint manager
Severity:	CVSS: 9.8 | EPSS: 0.106%
Type:	Remote code execution
Impact:	Confidentiality, integrity, availability
PoC:	Link
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Apply patch
MITRE advisory:	Read more

CVE-2024-29847 is a critical vulnerability in Ivanti Endpoint Manager (EPM) that allows remote code execution without authentication due to improper deserialization of untrusted data in the agent portal. It affects EPM versions 2024 (with September update) and earlier, enabling attackers to execute arbitrary code and potentially compromise networks. Ivanti has released updates for EPM 2022 and a security patch for EPM 2024, addressing this and 15 other vulnerabilities. Administrators should upgrade immediately to prevent exploitation, as no workarounds exist.

Summary

This report summarizes key vulnerabilities from Q3 2024, emphasizing the growing threats from state-sponsored attacks, ransomware, and widespread flaws in systems like PHP and OpenSSH. Critical vulnerabilities allowed for remote code execution and exploitation of network devices, with Iran-based ransomware groups being particularly active. Common attack vectors like SQL injections remained a persistent issue, especially in legacy systems, often exploited using automated tools.

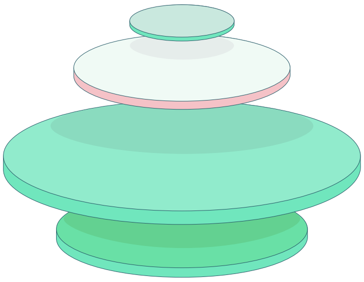
The events of Q3 2024 highlight the need for organizations to continuously update their systems, educate developers on secure coding practices, and strengthen their overall vulnerability management strategies.

About Vulcan Cyber

The Vulcan Cyber ExposureOS is the one platform for managing exposure risk across IT and cloud-native surfaces. At its core, the platform aggregates and correlates security findings from your infrastructure, code, application, and cloud environments into the exposure data lake. Vulcan Cyber then provides asset risk context, recommendations for the best fixes, and automated remediation workflows to streamline tedious mitigation tasks. Our commitment to innovation has earned recognition as a 2023 Forrester Wave Leader and Omdia RBVM leader. Prominent security teams, such as those at Mandiant and Snowflake, trust Vulcan Cyber to help them own their risk.

See Vulcan Cyber in action >>

Read our blog >>



Start owning your risk

Try Vulcan Free