Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti CSA Zero-Day Exploits Trigger Widespread Attacks

Date of Publication	Admiralty Code	TA Number
October 9, 2024	A1	TA2024385

Summary

First Seen: October 2024
Affected Products: Ivanti Cloud Service Appliance (CSA)
Impact: Ivanti has issued critical updates for its Cloud Services Appliance (CSA), addressing three zero-day vulnerabilities. These flaws, if exploited, could allow an attacker with administrative privileges to bypass security restrictions, execute arbitrary SQL commands, or achieve remote code execution (RCE). Notably, the zero-day vulnerabilities are being actively weaponized alongside a previously patched flaw, CVE-2024-8963, which was fixed last month. Given their active exploitation in attacks, users are strongly advised to apply the patches immediately to mitigate potential threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-9379	Ivanti Cloud Services Appliance SQL Injection Vulnerability	Ivanti Cloud Service Appliance (CSA)	✓	✓	✓
CVE-2024-9380	Ivanti Cloud Services Appliance OS Command Injection Vulnerability	Ivanti Cloud Service Appliance (CSA)	✓	✓	✓
CVE-2024-9381	Ivanti Cloud Services Appliance Path Traversal Vulnerability	Ivanti Cloud Service Appliance (CSA)	✓	✗	✓

Vulnerability Details

#1 Ivanti has issued an urgent warning regarding three newly discovered zero-day vulnerabilities CVE-2024-9379, CVE-2024-9380, and CVE-2024-9381 affecting its Cloud Services Appliance (CSA), which are currently under active exploitation. These zero-day flaws are being weaponized alongside a previously disclosed vulnerability, CVE-2024-8963, escalating the risk of attacks. These flaws were discovered while investigating the exploitation of CVE-2024-8963 and CVE-2024-8190 in CSA 4.6.

#2

The vulnerabilities target versions prior to 5.0.2 of the Ivanti CSA. CVE-2024-9379 is a SQL injection vulnerability that allows remote authenticated attackers with admin privileges to execute arbitrary SQL commands, potentially leading to system corruption. CVE-2024-9380 is an OS command injection flaw that enables attackers to gain remote code execution, posing the risk of complete system takeover. Lastly, CVE-2024-9381 is a path traversal vulnerability that allows attackers to bypass security restrictions and access unauthorized files. All three vulnerabilities have been observed in live attacks, emphasizing the need for immediate updates.

#3

A limited number of users running CSA version 4.6 patch 518 and earlier have already experienced security breaches through previous attacks. More recently, attackers have chained vulnerabilities CVE-2024-9379, CVE-2024-9380 and CVE-2024-8963, leading to further significant compromises. Ivanti strongly urges affected users to immediately restore their CSA appliances to version 5.0.2 to secure their systems and prevent further exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-9379	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	CWE-89
CVE-2024-9380	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	CWE-77
CVE-2024-9381	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	CWE-22

Recommendations

Update: Users are strongly urged to update to the latest fixed version of Ivanti's Cloud Services Appliance (CSA), which addresses the vulnerabilities. For all users still using CSA versions 5.0.1 and earlier, upgrading to version 5.0.2 is crucial to mitigate these vulnerabilities and protect against ongoing attacks.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Monitor for Unusual Activity: Continuously monitor Ivanti CSA logs for unusual access attempts, abnormal user behavior, or repeated login failures, which could indicate an exploit attempt. Configure alerts for irregular traffic patterns, sudden spikes in data transfer, or unauthorized changes to system configurations. Use an IDS/IPS to detect signs of exploitation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter
T1068 Exploitation for Privilege Escalation			

Patch Details

Users are strongly urged to update to CSA 5.0.2 version immediately, as this latest release addresses the vulnerabilities.

Link:
https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

References

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381?language=en_US

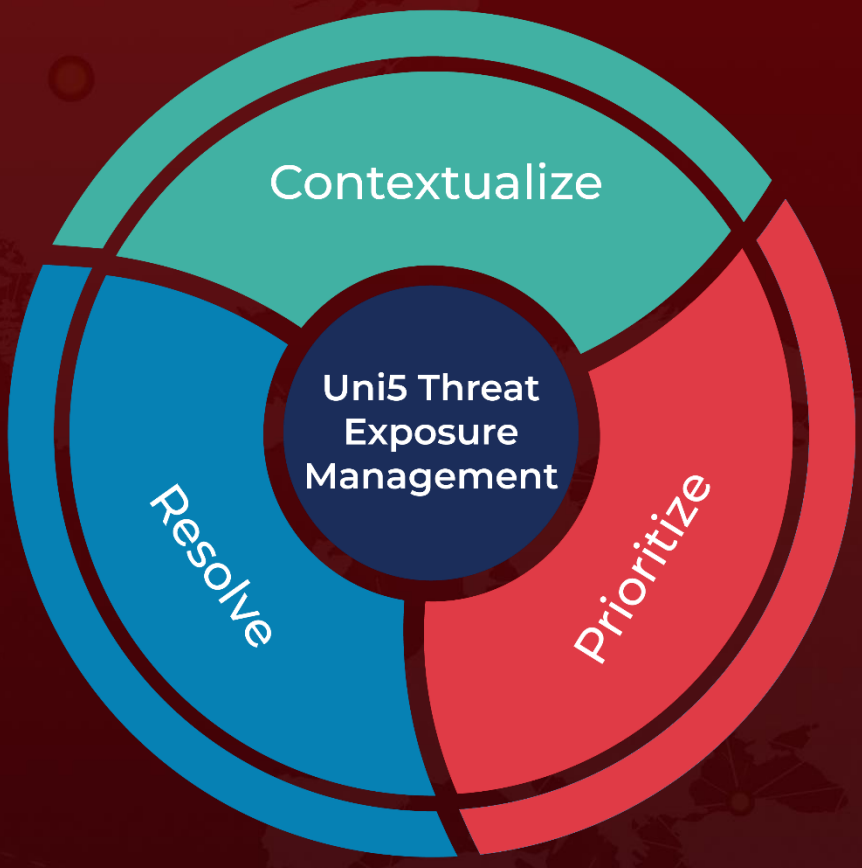
https://www.ivanti.com/blog/october-2024-security-update

https://hivepro.com/threat-advisory/ivanti-sounds-alarm-on-active-exploitation-of-flaw-in-cloud-service-appliance/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 9, 2024 . 6:00 AM

More at www.hivepro.com