Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti Sounds Alarm on Active Exploitation of Flaws in Cloud Service Appliance

Date of Publication	Last Update Date	Admiralty Code	TA Number
September 16, 2024	September 20, 2024	A1	TA2024356

Summary

First Seen: September 2024
Affected Products: Ivanti Cloud Service Appliance (CSA)
Impact: Ivanti has released a critical patch addressing two vulnerabilities, CVE-2024-8190 and CVE-2024-8963, impacting its Cloud Services Appliance (CSA). The first vulnerability allows a remote authenticated attacker to execute arbitrary commands on the system, potentially leading to full control through remote code execution (RCE). The second vulnerability is a path traversal flaw that permits a remote unauthenticated attacker to access restricted functionality. Alarmingly, both vulnerabilities have already been actively exploited in the wild. Users are strongly urged to apply the latest security updates immediately to mitigate these critical threats.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-8190	Ivanti Cloud Services Appliance OS Command Injection Vulnerability	Cloud Service Appliance (CSA)	✗	✓	✓
CVE-2024-8963	Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability	Cloud Services Appliance (CSA)	✗	✓	✓

Vulnerability Details

#1 Ivanti has issued a patch to address two critical vulnerabilities, CVE-2024-8190 and CVE-2024-8963, affecting its Cloud Services Appliance (CSA). This appliance is crucial for enabling secure, VPN-free communication between managed endpoints and corporate networks. Both vulnerabilities have already been actively exploited in the wild, making it imperative for users to update their systems immediately.

#2 CVE-2024-8190 stems from improper input validation, allowing privileged users to pass specially crafted data to execute OS-level commands on the Ivanti CSA. Although exploitation requires administrative access, systems configured with the recommended dual-homed setup—where ETH-0 is assigned to the internal network—are at significantly lower risk of compromise. However, despite this reduced risk, patching remains critical to ensure full protection.

#3 CVE-2024-8963 is a path traversal vulnerability that was disclosed after being incidentally addressed in the patch released on 10 September (CSA 4.6 Patch 519). This flaw allows remote, unauthenticated attackers to access restricted functionality on Ivanti's Cloud Services Appliance (CSA). When chained with CVE-2024-8190, it enables attackers to bypass admin authentication, ultimately allowing them to execute arbitrary commands on the appliance. This exploit chain poses a significant threat, potentially leading to full system compromise through remote code execution (RCE).

#4 Ivanti CSA 4.6 has reached End-of-Life and no longer receives security patches. While CSA 4.6 Patch 518 users can update to Patch 519, upgrading to CSA 5.0 is strongly recommended for continued security. To maintain support and protection, users must upgrade to Ivanti CSA 5.0, the only version that does not contain the vulnerabilities. Upgrading is crucial to staying protected against current and future threats.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-8190	CSA 4.6 (All versions before Patch 519)	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:patch_512:*:*:*:*:*:*:*	CWE- 78
CVE-2024-8963	CSA 4.6 (All versions before Patch 519)	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:patch_512:*:*:*:*:*:*:*	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 CVE-2024-8190 and CVE-2024-8963 vulnerabilities. Those still using the End-of-Life CSA 4.6 version should upgrade to the supported CSA 5.0 version immediately. This upgrade is essential for maintaining security, as CSA 5.0 is the only version that continues to receive updates and protection against these and future vulnerabilities.

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
TA0006 Credential Access	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	T1078 Valid Accounts	T1556 Modify Authentication Process

Patch Details

Users are strongly urged to update to CSA Patch 519 immediately, as this latest release addresses these vulnerabilities. The recommended long-term solution is to migrate to CSA 5.0, which continues to receive security updates and support.

Patch Links:
https://forums.ivanti.com/s/article/CSA-4-6-Patch-519

https://forums.ivanti.com/s/article/CSA-5-0-Download

References

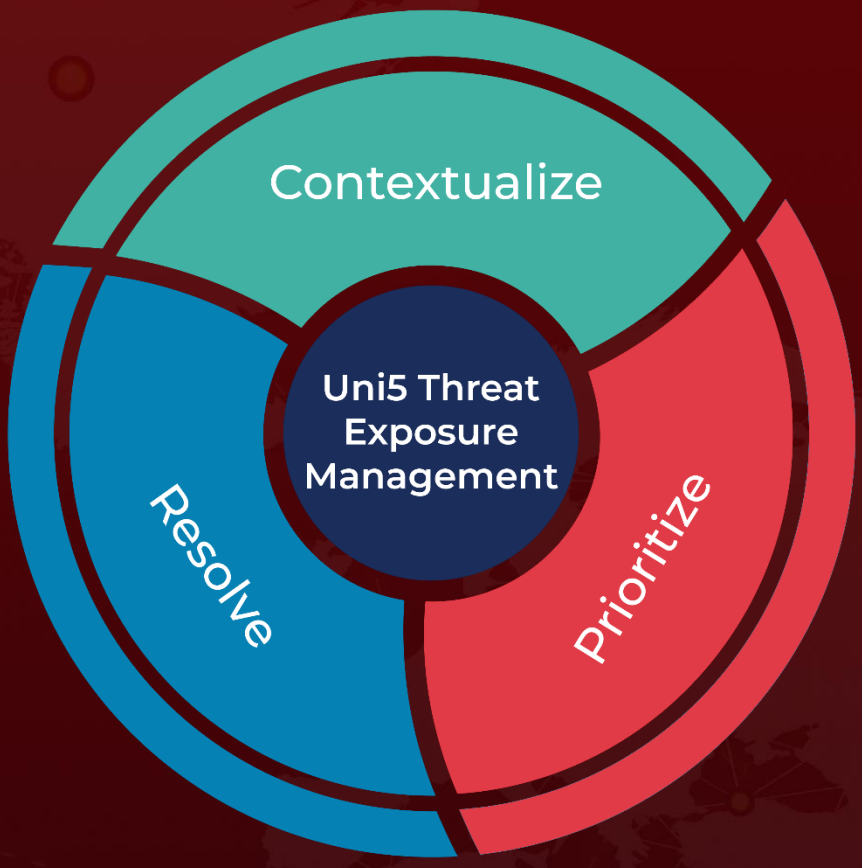
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190?

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963

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

September 16, 2024 • 7:00 AM

More at www.hivepro.com