

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Cisco Secure Client Flaw Enables Attackers To Steal VPN Sessions

Date of Publication

March 11, 2024

Admiralty Code

A1

TA Number

TA2024096




Summary

Discovered On: March 2024

Affected Products: Cisco Secure Client

Impact: A high severity vulnerability tracked as CVE-2024-20337 have been addressed by Cisco affecting its Secure Client software that could allow a threat actor to start a VPN session with the targeted user.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-20337	Cisco Secure Client Carriage Return Line Feed Injection Vulnerability	Cisco Secure Client			

Vulnerability Details

#1

Cisco has addressed a vulnerability, tracked as CVE-2024-20337, related to Carriage Return Line Feed (CRLF) injection attacks. This weakness in the Cisco Secure Client SAML authentication process could potentially be exploited by an unauthenticated remote attacker to start a VPN session with the targeted user.

#2

The CVE-2024-20337 vulnerability results from insufficient validation in the SAML authentication process, which allows a remote attacker to insert arbitrary data into a server response. An attacker can potentially compromise the integrity and security of the application by creating customized data that contains CR-LF characters.

#3

An attacker might leverage this issue to trick a user into opening a VPN session by having them click on a specially crafted link. If the exploit is successful, the attacker may be able to execute any script in the browser and obtain access to any private information kept there, including a valid SAML token.

#4

The attacker may then establish a remote access VPN session and utilize the rights of the compromised user by using the stolen token. Cisco has released software patches to address this vulnerability, with no workarounds provided. Versions prior to 4.10.04065 are not susceptible to this issue.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20337	Cisco Secure Client: 4.10.04065 - 5.1	cpe:2.3:a:cisco:CiscoSecure Client:*:*:*:*:*	CWE-93

Recommendations



Apply Patch: Install the security patch provided by Cisco to address the CVE-2024-20337 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.



Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.



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

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0006</u> Credential Access	<u>TA0007</u> Discovery	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities
<u>T1566</u> Phishing	<u>T1566.002</u> Spearphishing Link	<u>T1204</u> User Execution	<u>T1204.001</u> Malicious Link
<u>T1078</u> Valid Accounts	<u>T1217</u> Browser Information Discovery	<u>T1528</u> Steal Application Access Token	

Patch Details

Cisco has released patches to address the vulnerability CVE-2024-20337 in the latest versions. Upgrade to the version 4.10.08025 or version 5.1.2.42 or later.

Link:

<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/series.html#~tab-downloads>

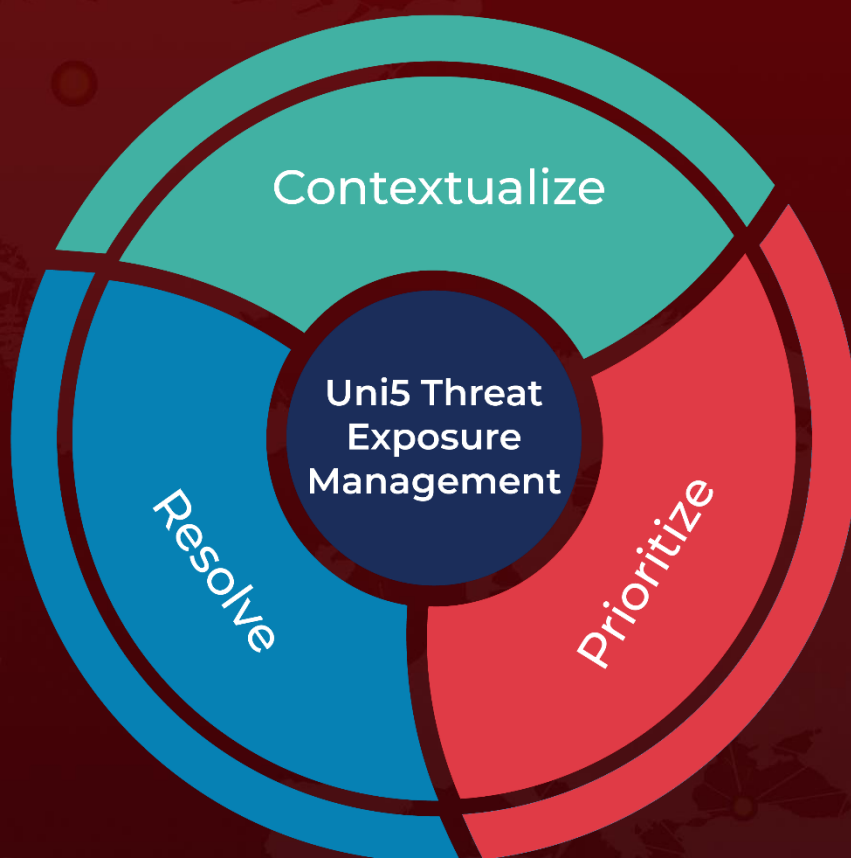
References

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7>

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

March 11, 2024 • 5:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com