Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Path Traversal Flaw in Splunk Enterprise Puts Windows Systems at Risk

Date of Publication	Admiralty Code	TA Number
July 23, 2024	A1	TA2024280

Summary

First Seen: July 2024
Affected Products: Splunk Enterprise on Windows
Impact: A high-severity vulnerability identified in Splunk, CVE-2024-36991, has been discovered. This vulnerability is associated with Path Traversal on the “/modules/messaging/” endpoint in Splunk Enterprise on Windows. It allows attackers to traverse the file system and access files or directories outside the restricted directory. A proof of concept for this vulnerability is publicly available on GitHub.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-36991	Splunk Enterprise Path Traversal Vulnerability	Splunk Enterprise	☒	☒	✓

Vulnerability Details

#1 A critical vulnerability, identified as CVE-2024-36991, has been detected in Splunk Enterprise, particularly impacting the “/modules/messaging/” endpoint on Windows. This flaw, rated 7.5 on the severity scale. Splunk Enterprise, a widely utilized tool for security and monitoring, allows organizations to search, analyze, and visualize data to enhance incident response.

#2 CVE-2024-36991 enables attackers to exploit the Windows implementation of Python's os.path.join function, allowing unauthorized directory listings and file reads on vulnerable Splunk instances with Splunk Web enabled. A crafted GET request to a vulnerable instance can exploit this flaw, as demonstrated by a proof of concept (PoC) that shows how attackers can traverse directories to access unauthorized files, potentially leading to sensitive data exposure.

#3

Over 230,000 internet-exposed servers running Splunk are vulnerable to this flaw. Users of affected Splunk Enterprise versions are strongly advised to upgrade to the latest versions—Splunk Enterprise 9.2.2, 9.1.5, 9.0.10, or higher—to mitigate this threat. As a temporary measure, administrators may limit the Splunk Web service exposure to more restricted network segments.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-36991	Splunk Enterprise Versions 9.2.0 to 9.2.1, 9.1.0 to 9.1.4, 9.0.0 to 9.0.9	cpe:2.3:a:splunk:splunk:*:*:*:*:enterprise:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	CWE-35

Recommendations

Update: Users are strongly advised to upgrade to the latest versions of Splunk Enterprise to mitigate the CVE-2024-36991 vulnerability. The recommended versions are Splunk Enterprise 9.2.2, 9.1.5, 9.0.10, or higher.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Sanitize Input Paths: Developers should rigorously validate and sanitize input paths to prevent unintended path traversal. Ensure that applications do not construct file paths using untrusted input without implementing proper checks.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0007 Discovery	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1083 File and Directory Discovery			

Patch Details

Users are strongly advised to upgrade to the latest versions of Splunk Enterprise to mitigate the CVE-2024-36991 vulnerability. The recommended versions are Splunk Enterprise 9.2.2, 9.1.5, 9.0.10, or higher.

Link: https://docs.splunk.com/Documentation/Splunk/9.2.2/ReleaseNotes/MeetSplunk

References

https://advisory.splunk.com/advisories/SVD-2024-0711

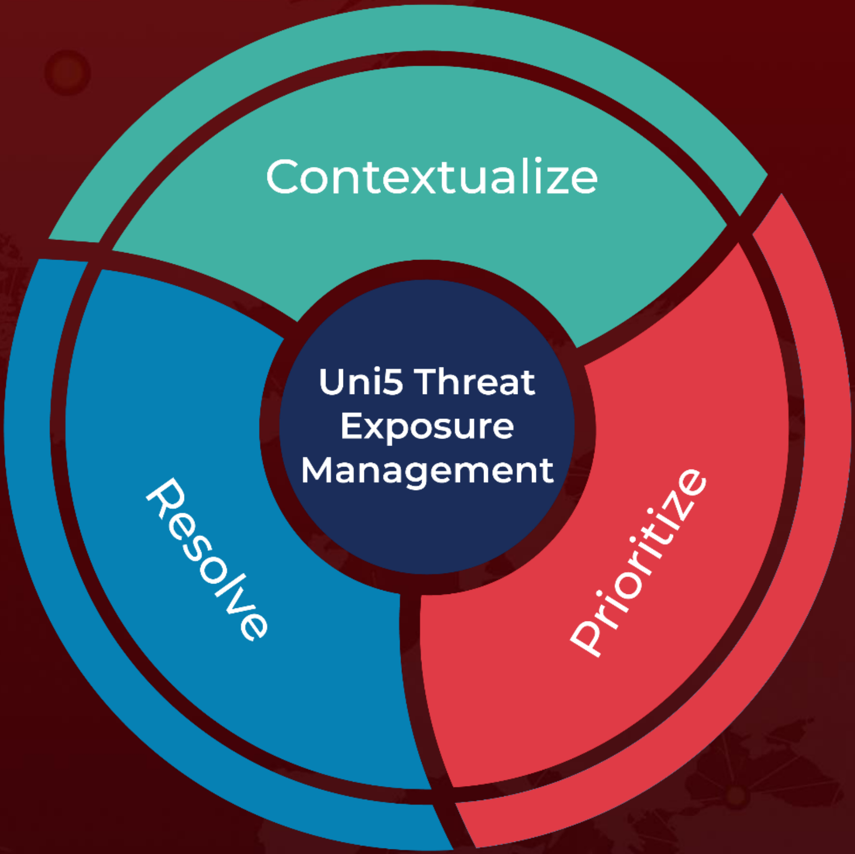
https://blog.sonicwall.com/en-us/2024/07/critical-splunk-vulnerability-cve-2024-36991-patch-now-to-prevent-arbitrary-file-reads/

https://github.com/bigb0x/CVE-2024-36991

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

July 23, 2024 • 8:00 AM

More at www.hivepro.com