Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

New Vulnerability Found in the JsonWebToken Open-Source Project

Date of Publication	Admiralty Code	TA Number
January 10, 2023	A1	TA2023015

Summary

First Seen: July 13, 2022
Affected Product: Devices that use an open-source JavaScript package JsonWebToken
Impact: Remote code execution can lead to the attacker gaining control of the compromised system.

CVEs

CVE	NAME	PATCH
CVE-2022-23529	JsonWebToken Remote Code Execution vulnerability	✓

Vulnerability Details

#1 A new high-severity vulnerability named CVE-2022-23529 has been discovered in the popular JsonWebToken open-source package. This vulnerability allows attackers to execute remote code on servers that verify a maliciously crafted JSON web token (JWT) request.

#2 The package had over 9 million weekly downloads and over 20,000 dependents at the time of discovery. JWT (JSON Web Token) is a standard for securely transmitting information by encoding and signing JSON data. It is used to transmit "claims", which are pieces of information about a subject, and are commonly used for authentication and authorization in many applications.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-23529	JsonWebToken	cpe:2.3:a:auth0:jsonwebtoken:*:*:*:*:*:node.js:*:*	CWE-20

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0042 Resource Development	TA0006 Credential Access	T1552.004 Unsecured Credentials: Private Keys	T1556 Modify Authentication Process
T1134 Access Token Manipulation	T1203 Exploitation for Client Execution	T1588.005 Exploits	T1552 Unsecured Credentials
T1588.006 Vulnerabilities	T1588 Obtain Capabilities		

Patch Details

Update to version 9.0.0 of the JsonWebToken package.

Links:
https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

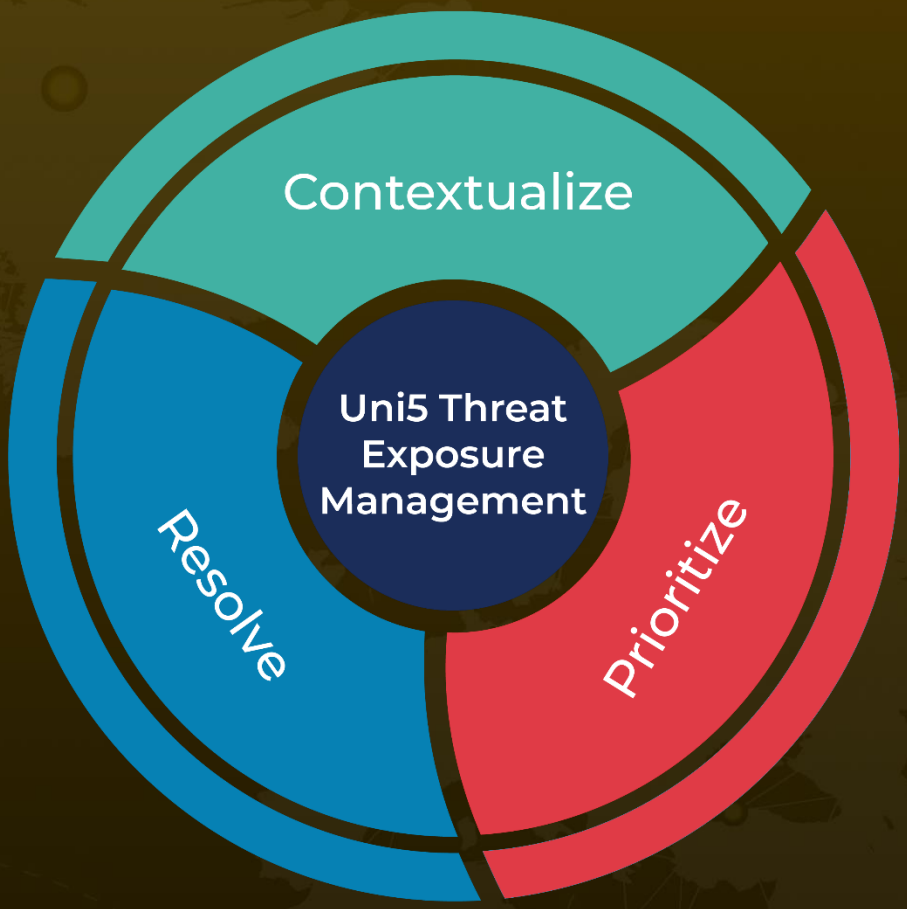
References

https://unit42.paloaltonetworks.com/jsonwebtoken-vulnerability-cve-2022-23529/

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

January 10, 2023 . 6:30 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com