Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Privilege Escalation in VMware spring-security

Date of Publication	Admiralty code	TA Number
November 1, 2022	A1	TA2022240

Summary

A vulnerability in VMware's Spring Security affects the mapping of permitted scope in spring-security-oauth2-client, allowing privilege escalation.

CVEs

CVE	NAME	PATCH
CVE-2022-31690	Privilege Escalation in VMware spring-security-oauth2-client	✓

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0008** Lateral Movement	**TA0004** Privilege Escalation	**T1134** Access Token Manipulation
T1210 Exploitation of Remote Services	**T1203** Exploitation for Client Execution	**T1068** Exploitation for Privilege Escalation	

Technical Details

This vulnerability occurs because spring-security-oauth2-client does not enforce security limitations effectively. A malicious attacker can alter a request initiated by the client via the browser to the Authorization Server if the server replies with an OAuth2 Access Token with an empty scope list on the subsequent instance to the token endpoint to get the access token, resulting in a privilege escalation on the subsequent approval

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-31690	Spring Security: 5.0.0 - 5.7.4	cpe:2.3:a:vmware:spring_security:-:*:*:*:*:*:*:*	CWE-264

Patch Details

Upgrade VMware Spring Security to 5.7.5 and 5.6.9

Links:
https://github.com/spring-projects/spring-security/releases/tag/5.7.5

https://github.com/spring-projects/spring-security/releases/tag/5.6.9

References

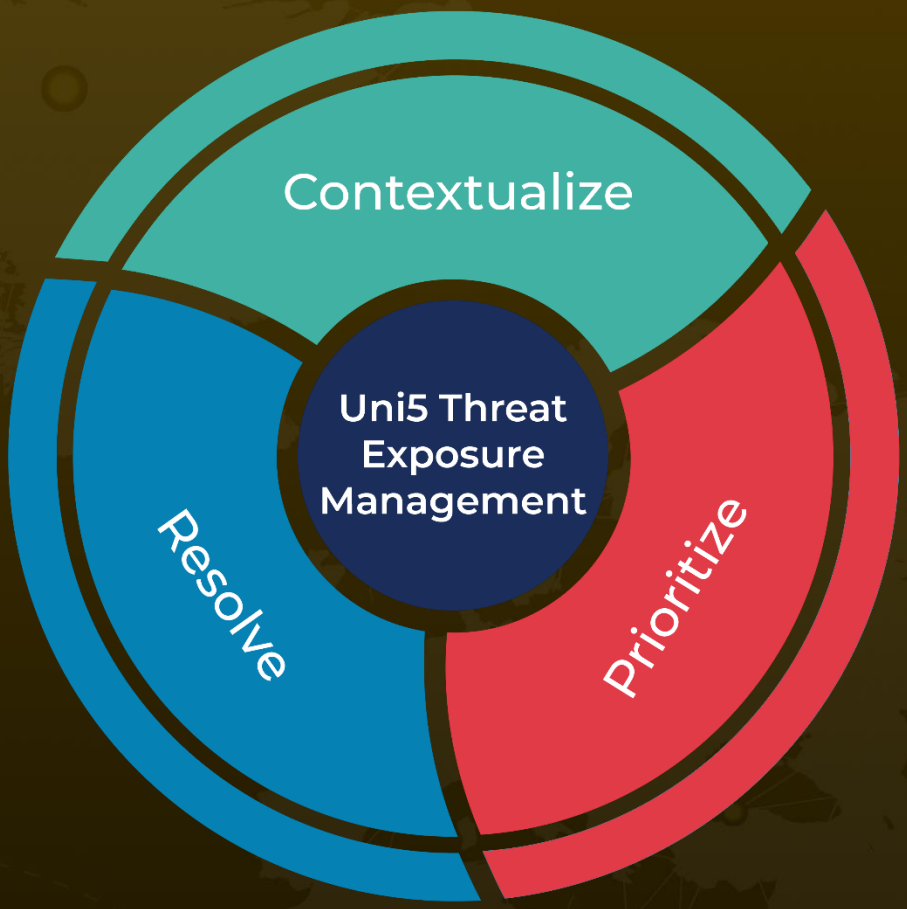
https://tanzu.vmware.com/security/cve-2022-31690

https://spring.io/blog

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 1, 2022 • 4:51 AM

More at www.hivepro.com