Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A Critical Vulnerability That Affects ManageEngine Products

Date of Publication	Last Update Date	Admiralty Code	TA Number
January 17, 2023	January 18, 2023	A1	TA2023026

Summary

First Seen: October 2022
Affected Product: ManageEngine products
Impact: The vulnerability allows for Remote code execution can lead to the attacker gaining control of the compromised system.

CVEs

CVE	NAME	PATCH
CVE-2022-47966	Remote code execution vulnerability in ManageEngine products	✓
CVE-2022-22972	Authentication bypass vulnerability in VMware products	✓
CVE-2022-28219	XXE vulnerability in Zoho ManageEngine ADAudit Plus	✓
CVE-2022-1388	Remote code execution vulnerability in F5 BIG-IP	✓

Vulnerability Details

#1

A critical vulnerability in several ManageEngine products allows for remote code execution (RCE) without authentication. This vulnerability is tracked as CVE-2022-47966 and is caused by an outdated third-party dependency, Apache Santuario. This vulnerability affects almost all ManageEngine products and allows unauthenticated attackers to execute arbitrary code if the SAML-based single-sign-on (SSO) is or was enabled at least once before the attack.

#2

Zoho has already patched the vulnerability by updating the third-party module to a more recent version. The researchers have created a proof-of-concept (PoC) exploit for the vulnerability and have warned that it is a good candidate for attackers to "spray and pray" across the internet. In addition to this, there are also a few other exploit codes that have been previously released by Horizon3.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-47966	ManageEngine products	cpe:2.3:a:manageengine:manageengine_access_manager_plus:4.3:4307:*:*:*:*:*:*	CWE-20
CVE-2022-22972	VMware Products	cpe:2.3:a:vmware:vmware_workspace_one_access:21.08.0.1:*:*:*:*:*:*:*	CWE-287
CVE-2022-28219	Zoho ManageEngine ADAudit Plus: 7000 - 7055	cpe:2.3:a:zohocorp:adaudit_plus:7055:*:*:*:*:*:*:*	CWE-611
CVE-2022-1388	BIG-IP: 11.6.1 - 16.1.2.1	cpe:2.3:h:f5_networks:big-ip:16.1.0:*:*:*:*:*:*:*	CWE-306

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' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution	TA0043 Reconnaissance
TA0003 Persistence	TA0042 Resource Development	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1203 Exploitation for Client Execution
T1509 Command and Scripting Interpreter			

Patch Links

https://www.manageengine.com/products/active-directory-audit/cve-2022-28219.html

https://www.vmware.com/security/advisories/VMSA-2022-0014.html

https://support.f5.com/csp/article/K23605346

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

References

https://www.bleepingcomputer.com/news/security/researchers-to-release-poc-exploit-for-critical-zoho-rce-bug-patch-now/

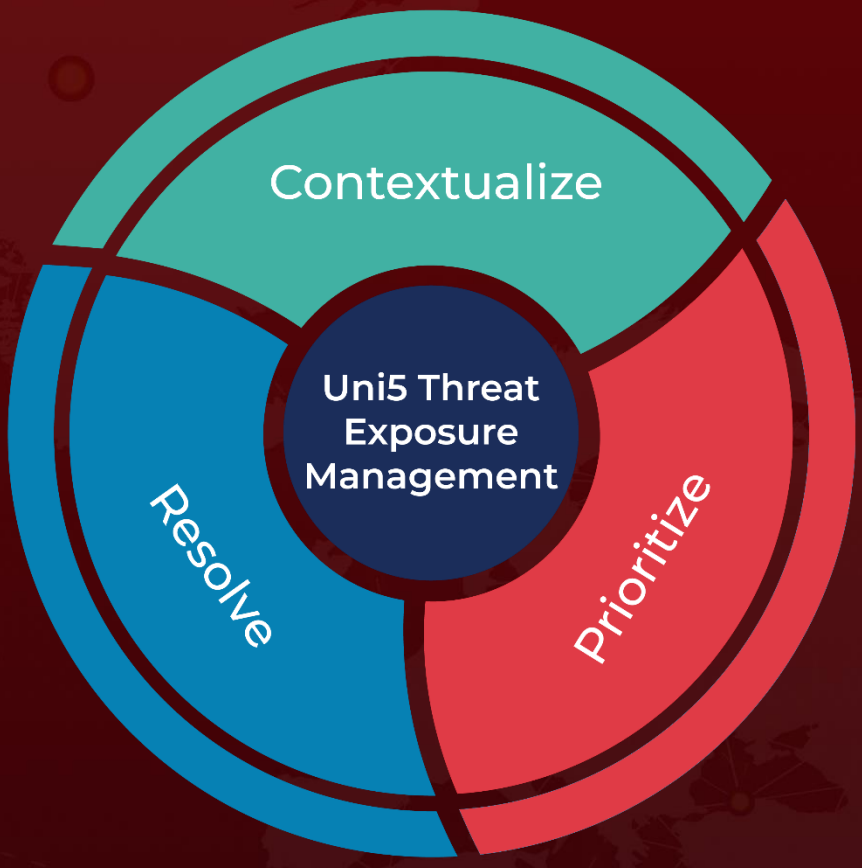
https://twitter.com/Horizon3Attack/status/1613380836660748288

https://twitter.com/Horizon3Attack/status/1613927091426451456

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 17, 2023 . 1:00 AM

More at www.hivepro.com