Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zoho Addresses SQL Injection Vulnerability in ManageEngine Products

Date of Publication	Admiralty Code	TA Number
January 5, 2023	A1	TA2023008

Summary

First Seen: December 30, 2022
Affected Products: Password Manager Pro, PAM360, and Access Manager Plus.
Impact: SQL injection by an unauthenticated attacker.

CVE

CVE	NAME	PATCH
CVE-2022-47523	SQL Injection Vulnerability in Zoho	✓

Vulnerability Details

A security flaw affecting multiple ManageEngine products identified as CVE-2022-47523 is an SQL injection vulnerability found in the ZOHO's Password Manager Pro Secure Vault, PAM360 Privileged Access Management Software, and Access Manager Plus Privileged Session Management Solution. If exploited, the vulnerability would allow attackers to gain unauthenticated access to the backend database and execute custom queries to access database table entries. Zoho has fixed the issue and is urging customers to upgrade to the latest builds of the affected products immediately.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-47523	Password Manager Pro version below: 12200, PAM360 version below: 5800, & Access Manager Plus version below: 4308	cpe:2.3:a:manageengine:manageengine_access_manager_plus:-:*:*:*:*:*:* cpe:2.3:a:manageengine:manageengine_PAM360:-:*:*:*:*:*:* cpe:2.3:a:manageengine:manageengine_password_manager_pro:-:*:*:*:*:*:*	CWE-89

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0008 Lateral Movement	TA0009 Collection	TA0040 Impact	T1190 Exploit Public-Facing Application
T1505 Server Software Component	T1505.003 Web Shell	T1136 Create Account	T1059 Command and Scripting Interpreter
T1005 Data from Local System	T1565 Data Manipulation	T1565.001 Stored Data Manipulation	

Patch Links

https://www.manageengine.com/privileged-session-management/advisory/cve-2022-47523.html

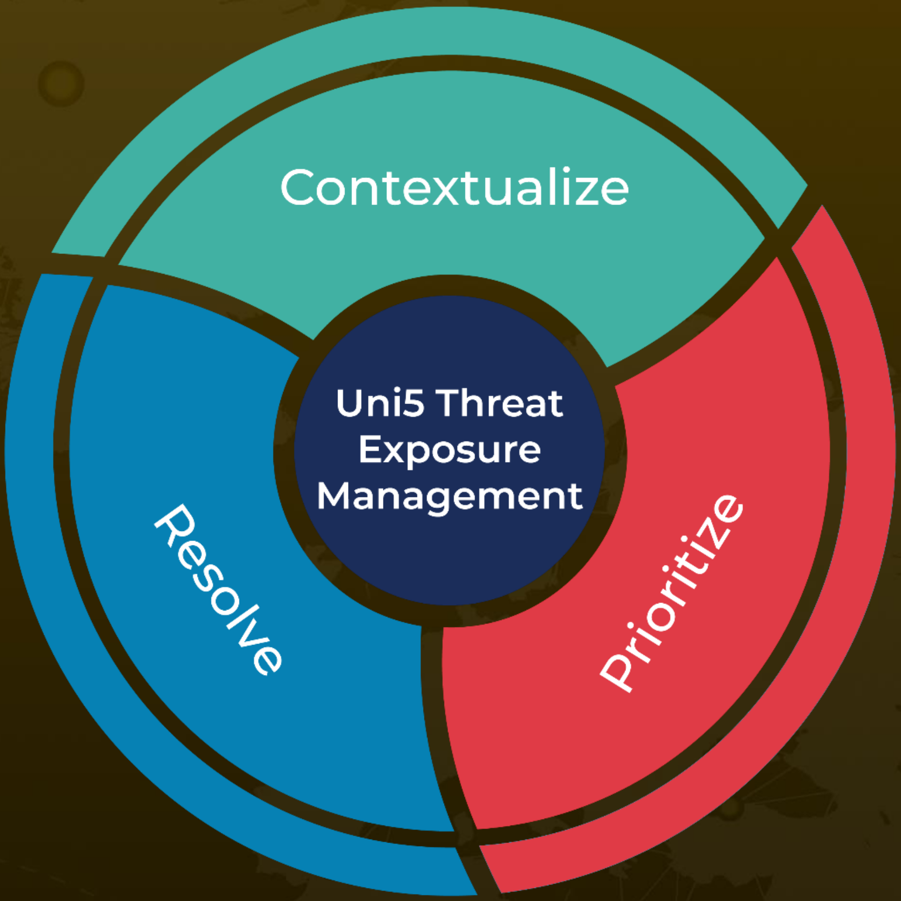
References

https://www.bleepingcomputer.com/news/security/zoho-urges-admins-to-patch-critical-manageengine-bug-immediately/?traffic_source=Connatix

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 5, 2023 • 3:33 AM

More at www.hivepro.com