AttackerKB sunset on August 18. Read our blog.

ATTACKER VALUE
VERY HIGH
(2 users assessed)

EXPLOITABILITY
MODERATE
(2 users assessed)

3

USER INTERACTION
None

CVE-2022-47966

Disclosure Date: January 18, 2023 · (Last upd

CVE-2022-47966 CVSS v3 Base Score: 9.8

Exploited in the Wild

Reported by mkienow-r7 and 4 more...
View Source Details

Report As Exploited in the Wild

MITRE ATT&CK

Log in to add MITRE ATT&CK tag

Add MITRE ATT&CK tactics and techniques that apply to this CVE.

Initial Access

TECHNIQUES	VALIDATION
Exploit Public-Facing Application	VALIDATED

Metasploit Module

exploit/windows/http/manageengine_endpoint_central_saml...
exploit/multi/http/manageengine_servicedesk_plus_saml_rce...
exploit/multi/http/manageengine_adselfservice_plus_saml_rc...

Watch This Topic

Watch this topic to be notified when new information, assessments, and comments are added

Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

I AGREE, LET'S GO!

View our Cookie Policy for full details

CISA KEV Listed | Common in enterprise | Easy to weaponize | Gives privileged access | Observed in ransomware attacks | Observed in state-sponsored attacks | Unauthenticated | Difficult to weaponize | Vulnerable in uncommon configuration

Description

Multiple Zoho ManageEngine on-premise products, such as ServiceDesk Plus through 14003, allow remote code execution due to use of Apache Santuario xmlsec (aka XML Security for Java) 1.4.1, because the xmlsec XSLT features, by design in that version, make the application responsible for certain security protections, and the ManageEngine applications did not provide those protections. This affects Access Manager Plus before 4308, Active Directory 360 before 4310, ADAudit Plus before 7081, ADManager Plus before 7162, ADSelfService Plus before 6211, Analytics Plus before 5150, Application Control Plus before 10.1.2220.18, Asset Explorer before 6983, Browser Security Plus before 11.1.2238.6, Device Control Plus before 10.1.2220.18, Endpoint Central before 10.1.2228.11, Endpoint Central MSP before 10.1.2228.11, Endpoint DLP before 10.1.2137.6, Key Manager Plus before 6401, OS Deployer before 1.1.2243.1, PAM 360 before 5713, Password Manager Pro before 12124, Patch Manager Plus before 10.1.2220.18, Remote Access Plus before 10.1.2228.11, Remote Monitoring and Management (RMM) before 10.1.41, ServiceDesk Plus before 14004, ServiceDesk Plus MSP before 13001, SupportCenter Plus before 11026, and Vulnerability Manager Plus

See More

Ratings & Analysis | Vulnerability Details | RAPID7 Analysis

ATTACKER VALUE
VERY HIGH

3

CVE-2022-47966

This site uses cookies for anonymized analytics. For more information or to change your cookie settings, view our Cookie Policy.