Zoho Exploit

Exploiting CVE-40539 in Zoho ManageEngine ServiceDesk Plus

https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

CVEs: CVE-2021-44077

APT Actors are actively exploiting Zoho ManageEngine ServiceDesk Plus which is an IT help desk software with asset management. The exploit is tracked via CVE-2021-44077 and rated critical due to its capability for unauthenticated remote code execution (RCE).

Background

The ManageEngine ServiceDesk Plus released a security advisory on authentication bypass vulnerability.

Announced

Dec 2: CISA and FBI released an alert on active exploitation

https://us-cert.cisa.gov/ncas/current-activity/2021/12/02/cisa-and-fbi-release-alert-active-exploitation-cve-2021-44077-zoho

https://us-cert.cisa.gov/ncas/alerts/aa21-336a

Dec 6: FortiGuard Labs published a threat signal report

https://www.fortiguard.com/threat-signal-report/4329/joint-cybersecurity-advisory-on-attacks-exploiting-zoho-manageengine-servicedesk-plus-vulnerability-cve-2021-44077

Latest Developments

On 2nd of December 2021, CISA has announced active exploitation of CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus. Based on FortiGuard statistics from the last few days, Malware using this vulnerability is active in the wild.

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiClient	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiEDR	AV (Pre-Filter)	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiSandbox	AV (Pre-Filter)	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiAI	AV (Pre-Filter)	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiMail	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiCASB	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiCWP	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiADC	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiProxy	AV	*89.07442*	Blocks exploitation of the Zoho vulnerability
FortiAnalyzer	Event Handlers & Reports	*6.4+*	Detects indicators for the Zoho vulnerability from across the security fabric
FortiSIEM	Rules & Reports	*6.0+*	Detects indicators for the Zoho vulnerability from across the security fabric and 3rd party products

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiClient
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiEDR
AV (Pre-Filter)
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiSandbox
AV (Pre-Filter)
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiAI
AV (Pre-Filter)
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiMail
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiCASB
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiCWP
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiADC
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

FortiProxy
AV
Version Info: 89.07442
Link: https://www.fortiguard.com/updates/antivirus?version=89.07442

Exploitation

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
Event Handlers & Reports
Version Info: 6.4+
Link:

FortiSIEM
Rules & Reports
Version Info: 6.0+
Link: