Hive Pro

THREAT ADVISORY

Zoho ManageEngine Desktop Central affected by critical vulnerability

TA2022013

Threat Level AMBER

Publish Date – Jan 19, 2022

Zoho has patched a critical vulnerability (CVE-2021-44757) in Desktop Central and Desktop Central MSP which are unified endpoint management (UEM) solutions.

A security vulnerability exists in the Desktop Central and Desktop Central MSP that allows a remote user to bypass the authentication mechanism. Successful exploitation of this issue may allow an attacker to read unauthorized data or write an arbitrary zip file on the server.

Similar Zoho ManageEngine vulnerability were primarily targeted by many APT groups in the year 2021. Around 2,800 ManageEngine Desktop central instances were found to be exposed in a Shodan search. Hive Pro researcher strongly recommends that affected customers upgrade to a fixed version before any exploitation occur.

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-44757	Zoho ManageEngine Desktop Central MSP: before 10.1.2137.9 and Zoho ManageEngine Desktop Central from versions 10.1.2119.8 to 10.1.2137.3	cpe:2.3:a:zohocorp:zoho_manage engine_desktop_central :*:*:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:zoho_manage engine_desktop_centra_Msp :*:*:*:*:*:*:*:*:*,	Zoho ManageEngine Desktop Central and Desktop Central MSP security bypass	CWE-287

Patch Link

https://pitstop.manageengine.com/portal/en/community/topic/a-critical-security-patch-released-in-desktop-central-and-desktop-central-msp-for-cve-2021-44757-17-1-2022

References

https://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html
https://securityaffairs.co/wordpress/126821/hacking/wordpress-plugins-flaws-2.html?utm_source=rss&utm_medium=rss&utm_campaign=wordpress-plugins-flaws-2
https://www.bleepingcomputer.com/news/security/zoho-plugs-another-critical-security-hole-in-desktop-central/