Hive Pro

THREAT ADVISORY

Several Zoho ManageEngine products have been exploited

TA202154

Threat Level RED

Publish Date – Dec 5, 2021

Multiple vulnerabilities have been discovered in Zoho ManageEngine products. The affected products include Zoho ManageEngine ServiceDesk Plus , Zoho ManageEngine SupportCenter Plus, Zoho ManageEngine Desktop Central, Zoho ManageEngine AssetExplorer.

CVE-2021-44077 is a vulnerability that could allow an attacker to run arbitrary code. It was discovered on November 20, 2021. This vulnerability, however, may be easily fixed by updating to Zoho version 11306, which was released in September. Attackers are focusing on the healthcare, financial services, electronics, and IT consulting businesses by exploiting this vulnerability.

CVE-2021-44515 & CVE-2021-44526 are authentication bypass vulnerabilities. CVE-2021-44515 only affects Zoho ManageEngine ServiceDesk and Zoho ManageEngine AssetExplorer who uses Desktop Central Agent for asset discovery and CVE-2021-44526 affects all vulnerable versions of Zoho ManageEngine ServiceDesk and Zoho ManageEngine AssetExplorer.

Two of these vulnerabilities (CVE-2021-44077 and CVE-2021-44515)have been exploited in the wild so organizations should upgrade their Zoho ManageEngine products to their latest versions to eliminate these vulnerabilities.

The Techniques used by an unknown actor to exploit CVE-2021-44077 includes:

T1190 - Exploit Public-Facing Application
T1505.003 - Server Software Component: Web Shell
T1027 - Obfuscated Files or Information
T1140 - Deobfuscate/Decode Files or Information
T1003 - OS Credential Dumping
T1218 - Signed Binary Proxy Execution
T1136 - Create Account
T1003.003 - OS Credential Dumping: NTDS
T1047 - Windows Management Instrumentation
T1070.004 - Indicator Removal on Host: File Deletion
T1087.002 - Account Discovery: Domain Account
T1560.001 - Archive Collected Data: Archive via Utility
T1573.001 - Encrypted Channel: Symmetric Cryptography

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name
CVE-2021-44077 (CWE-287)	Zoho ManageEngine ServiceDesk Plus version up to 11305 , ServiceDesk Plus MSP version up to 10529 , SupportCenter Plus version up to 11013	cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:*:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_servicedesk_plus_msp:*:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_supportcenter_plus:*:*:*:*:*:*:*:*	Zoho ManageEngine unauthenticated remote code execution vulnerability
CVE-2021-44515	Zoho ManageEngine Desktop Central version 10.1.2127.17 and below and 10.1.2128.0 to 10.1.2137.2, AssetExplorer versions up to 6952	cpe:2.3:a:zohocorp:manageengine_desktop_central:-:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_assetexplorer:-:*:*:*:*:*:*:*	An authentication bypass vulnerability in ManageEngine Desktop Central
CVE-2021-44526	Zoho ManageEngine ServiceDesk Plus versions 12002 and below, AssetExplorer versions up to 6952	cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:*:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_assetexplorer:-:*:*:*:*:*:*:*	An authentication bypass vulnerability in ServiceDesk Plus

Indicators of Compromise(IoCs) *

Type	Value
Hashes	67ee552d7c1d46885b91628c603f24b66a9755858e098748f7e7862a71baa015 068D1B3813489E41116867729504C40019FF2B1FE32AAB4716D429780E666324 759bd8bd7a71a903a26ac8d5914e5b0093b96de61bf5085592be6cc96880e088 262cf67af22d37b5af2dc71d07a00ef02dc74f71380c72875ae1b29a3a5aa23d a44a5e8e65266611d5845d88b43c9e4a9d84fe074fd18f48b50fb837fa6e429d ce310ab611895db1767877bd1f635ee3c4350d6e17ea28f8d100313f62b87382 75574959bbdad4b4ac7b16906cd8f1fd855d2a7df8e63905ab18540e2d6f1600 5475aec3b9837b514367c89d8362a9d524bfa02e75b85b401025588839a40bcb Ecd8c9967b0127a12d6db61964a82970ee5d38f82618d5db4d8eddbb3b5726b7 009d23d85c1933715c3edcccb46438690a66eebbcccb690a7b27c9483ad9d0ac 083bdabbb87f01477f9cf61e78d19123b8099d04c93ef7ad4beb19f4a228589a 342e85a97212bb833803e06621170c67f6620f08cc220cf2d8d44dff7f4b1fa3 805b92787ca7833eef5e61e2df1310e4b6544955e812e60b5f834f904623fd9f 3da8d1bfb8192f43cf5d9247035aa4445381d2d26bed981662e3db34824c71fd 5b8c307c424e777972c0fa1322844d4d04e9eb200fe9532644888c4b6386d755 3f868ac52916ebb6f6186ac20b20903f63bc8e9c460e2418f2b032a207d8f21d 342a6d21984559accbc54077db2abf61fd9c3939a4b09705f736231cbc7836ae 7e4038e18b5104683d2a33650d8c02a6a89badf30ca9174576bf0aff08c03e72 3c90df0e02cc9b1cf1a86f9d7e6f777366c5748bd3cf4070b49460b48b4d4090 b4162f039172dcb85ca4b85c99dd77beb70743ffd2e6f9e0ba78531945577665 E391c2d3e8e4860e061f69b894cf2b1ba578a3e91de610410e7e9fa87c07304c Bec067a0601a978229d291c82c35a41cd48c6fca1a3c650056521b01d15a72da D0c3d7003b7f5b4a3bd74a41709cfecfabea1f94b47e1162142de76aa7a063c7 7d2780cd9acc516b6817e9a51b8e2889f2dec455295ac6e6d65a6191abadebff
Filepaths	C:\ManageEngine\ServiceDesk\bin\msiexec.exe C:\ManageEngine\ServiceDesk\lib\tomcat\tomcat-postgres.jar C:\Windows\Temp\ScriptModule.dll C:\ManageEngine\ServiceDesk\bin\ScriptModule.dll C:\Windows\system32\ME_ADAudit.exe c:\Users\[username]\AppData\Roaming\ADManager\ME_ADManager.exe %ALLUSERPROFILE%\Microsoft\Windows\Caches\system.dat C:\ProgramData\Microsoft\Crypto\RSA\key.dat c:\windows\temp\ccc.exe
Domains	seed.nkn[.]org

Patch Links

https://www.manageengine.com/desktop-management-msp/cve-2021-44515-security-advisory.html
https://www.manageengine.com/products/service-desk/security-response-plan.html
https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44526-and-cve-2021-44515-authentication-bypass-vulnerabilities-in-servicedesk-plus-and-desktop-central
https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44526-and-cve-2021-44515-authentication-bypass-vulnerabilities-in-assetexplorer-and-desktop-central

References

https://us-cert.cisa.gov/ncas/alerts/aa21-336a
https://www.bleepingcomputer.com/news/security/zoho-patch-new-manageengine-bug-exploited-in-attacks-asap/
https://unit42.paloaltonetworks.com/tiltedtemple-manageengine-servicedesk-plus/

*** Indicates parameters that apply to CVE-2021-44077**