



Attackers Exploiting Zoho ManageEngine

CRITICALITY



10/11/2021

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A pre-auth vulnerability affects Zoho ManageEngine ADSelfService Plus is currently being exploited in the wild, and the company recommends all the customers to keep the product up to date.



Threat Details

On Sept 2021, the US Cybersecurity and Infrastructure Security Agency (CISA) released a warning about APT actors were actively exploiting CVE-2021-40539 bypass authentication vulnerability in ManageEngine ADSelfService Plus. Nowadays, a second campaign is observed exploiting the same vulnerability.

Successful exploitation of the vulnerability will allow the attacker to upload Godzilla webshell, NGLite backdoor, Dropper, and KdcSponge the new credential-stealer. Consequently, the attacker retains persistent access on the network and gathers credentials from the Active Directory server.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

Robert Falcone, J. W. (2021, November 7). *Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer*. Retrieved from Palo Alto Networks: <https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdc sponge/>

Vaas, L. (2021, November 8). *Zoho Password Manager Flaw Torched by Godzilla Webshell*. Retrieved from threat post: <https://threatpost.com/zoho-password-manager-flaw-godzilla-webshell/176063/>



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities follow the below steps to help organizations thwart these attacks:

- Update ADSelfService Plus version to the latest version.
- Make sure that ADSelfService Plus is not directly accessible from the internet.
- As mentioned by the company, even those versions that are not yet affected must have the latest version installed.

Affected products:

- Zoho ManageEngine ADSelfService Plus builds 6113 and below.



Appendix B – Detection

Indicators of Compromise

Hashes – SHA256

Dropper	b2a29d99a1657140f4e254221d8666a736160ce960d06557778318e0d1b7423b5fcc9f3b514b853e8e9077ed4940538aba7b3044edbbba28ca92ed37199292058
NGLite	805b92787ca7833eef5e61e2df1310e4b6544955e812e60b5f834f904623fd9f3da8d1bfb8192f43cf5d9247035aa4445381d2d26bed981662e3db34824c71fd5b8c307c424e777972c0fa1322844d4d04e9eb200fe9532644888c4b6386d7553f868ac52916ebb6f6186ac20b20903f63bc8e9c460e2418f2b032a207d8f21d
Godzilla Webshell	a44a5e8e65266611d5845d88b43c9e4a9d84fe074fd18f48b50fb837fa6e429dce310ab611895db1767877bd1f635ee3c4350d6e17ea28f8d100313f62b8738275574959bbdad4b4ac7b16906cd8f1fd855d2a7df8e63905ab18540e2d6f16005475aec3b9837b514367c89d8362a9d524bfa02e75b85b401025588839a40bcb
KdcSponge	3c90df0e02cc9b1cf1a86f9d7e6f777366c5748bd3cf4070b49460b48b4d4090b4162f039172dcb85ca4b85c99dd77beb70743ffd2e6f9e0ba78531945577665

IP Addresses

- 24.64.36[.]238
- 45.63.62[.]109
- 45.76.173[.]103
- 45.77.121[.]232
- 66.42.98[.]156
- 140.82.17[.]161
- 149.28.93[.]184
- 149.248.11[.]205
- 199.188.59[.]192

Registry Keys

- Software\Microsoft\Windows\CurrentVersion\Run\ME_ADManager.exe
- Software\Microsoft\Windows\CurrentVersion\Run\ME_ADAudit.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\KDC Service



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.