APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus

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

Summary

This joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 9. See the ATT&CK for Enterprise framework for referenced threat actor techniques and for mitigations.

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of a newly identified vulnerability (CVE-2021-44077) in Zoho ManageEngine ServiceDesk Plus—IT help desk software with asset management.

CVE-2021-44077, which Zoho rated critical, is an unauthenticated remote code execution (RCE) vulnerability affecting all ServiceDesk Plus versions up to, and including, version 11305. This vulnerability was addressed by the update released by Zoho on September 16, 2021 for ServiceDesk Plus versions 11306 and above. The FBI and CISA assess that advanced persistent threat (APT) cyber actors are among those exploiting the vulnerability. Successful exploitation of the vulnerability allows an attacker to upload executable files and place webshells, which enable the adversary to conduct post-exploitation activities, such as compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files.

The Zoho update that patched this vulnerability was released on September 16, 2021, along with a security advisory. Additionally, an email advisory was sent to all ServiceDesk Plus customers with additional information. Zoho released a subsequent security advisory on November 22, 2021, and advised customers to patch immediately.

The FBI and CISA are aware of reports of malicious cyber actors likely using exploits against CVE-2021-44077 to gain access [T1190] to ManageEngine ServiceDesk Plus, as early as late October 2021. The actors have been observed using various tactics, techniques and procedures (TTPs), including:

- Writing webshells [T1505.003] to disk for initial persistence
- Obfuscating and Deobfuscating/Decoding Files or Information [T1027 and T1140]
- Conducting further operations to dump user credentials [T1003]
- Living off the land by only using signed Windows binaries for follow-on actions [T1218]
- Adding/deleting user accounts as needed [T1136]

- Stealing copies of the Active Directory database (`NTDS.dit`) [T1003.003] or registry hives
- Using Windows Management Instrumentation (WMI) for remote execution [T1047]
- Deleting files to remove indicators from the host [T1070.004]
- Discovering domain accounts with the net Windows command [T1087.002]
- Using Windows utilities to collect and archive files for exfiltration [T1560.001]
- Using custom symmetric encryption for command and control (C2) [T1573.001]

The FBI and CISA are proactively investigating this malicious cyber activity:

- The FBI leverages specially trained cyber squads in each of its 56 field offices and CyWatch, the FBI's 24/7 operations center and watch floor, which provides around-the-clock support to track incidents and communicate with field offices across the country and partner agencies.
- CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

Sharing technical and/or qualitative information with the FBI and CISA helps empower and amplify our capabilities as federal partners to collect and share intelligence and engage with victims, while working to unmask and hold accountable those conducting malicious cyber activities.

Click here for a PDF version of this report.

Click here for indicators of compromise (IOCs) in STIX format.

Technical Details

Compromise of the affected systems involves exploitation of CVE-2021-44077 in ServiceDesk Plus, allowing the attacker to:

1. Achieve an unrestricted file upload through a POST request to the ServiceDesk REST API URL and upload an executable file, `C:\ManageEngine\Servicedesk\bin\msiexec.exe` , with a SHA256 hash of `ecd8c9967b0127a12d6db61964a82970ee5d38f82618d5db4d8eddbb3b5726b7` . This executable file serves as a dropper and contains an embedded, encoded Godzilla JAR file.
2. Gain execution for the dropper through a second POST request to a different REST API URL, which will then decode the embedded Godzilla JAR file and drop it to the filepath `C:\ManageEngine\ServiceDesk\lib\tomcat\tomcat-postgres.jar` with a SHA256 hash of `67ee552d7c1d46885b91628c603f24b66a9755858e098748f7e7862a71baa015` .

Confirming a successful compromise of ManageEngine ServiceDesk Plus may be difficult—the attackers are known to run clean-up scripts designed to remove traces of the initial point of compromise and hide any relationship between exploitation of the vulnerability and the webshell.

Targeted Industries

APT cyber actors have targeted Critical Infrastructure Sector industries, including the healthcare, financial services, electronics and IT consulting industries.

Indicators of Compromise

Hashes

Webshell:

```
67ee552d7c1d46885b91628c603f24b66a9755858e098748f7e7862a71baa015
068D1B3813489E41116867729504C40019FF2B1FE32AAB4716D429780E666324
759bd8bd7a71a903a26ac8d5914e5b0093b96de61bf5085592be6cc96880e088
262cf67af22d37b5af2dc71d07a00ef02dc74f71380c72875ae1b29a3a5aa23d
a44a5e8e65266611d5845d88b43c9e4a9d84fe074fd18f48b50fb837fa6e429d
ce310ab611895db1767877bd1f635ee3c4350d6e17ea28f8d100313f62b87382
75574959bbdad4b4ac7b16906cd8f1fd855d2a7df8e63905ab18540e2d6f1600
5475aec3b9837b514367c89d8362a9d524bfa02e75b85b401025588839a40bcb
```

Dropper:

```
ecd8c9967b0127a12d6db61964a82970ee5d38f82618d5db4d8eddbb3b5726b7
```

Implant:

```
009d23d85c1933715c3edcccb46438690a66eebbcccb690a7b27c9483ad9d0ac
083bdabbb87f01477f9cf61e78d19123b8099d04c93ef7ad4beb19f4a228589a
342e85a97212bb833803e06621170c67f6620f08cc220cf2d8d44dff7f4b1fa3
```

NGLite Backdoor:

```
805b92787ca7833eef5e61e2df1310e4b6544955e812e60b5f834f904623fd9f
3da8d1bfb8192f43cf5d9247035aa4445381d2d26bed981662e3db34824c71fd
5b8c307c424e777972c0fa1322844d4d04e9eb200fe9532644888c4b6386d755
3f868ac52916ebb6f6186ac20b20903f63bc8e9c460e2418f2b032a207d8f21d
342a6d21984559accbc54077db2abf61fd9c3939a4b09705f736231cbc7836ae
7e4038e18b5104683d2a33650d8c02a6a89badf30ca9174576bf0aff08c03e72
```

KDC Sponge:

```
3c90df0e02cc9b1cf1a86f9d7e6f777366c5748bd3cf4070b49460b48b4d4090
b4162f039172dcb85ca4b85c99dd77beb70743ffd2e6f9e0ba78531945577665
e391c2d3e8e4860e061f69b894cf2b1ba578a3e91de610410e7e9fa87c07304c
```

Malicious IIS Module:

`bec067a0601a978229d291c82c35a41cd48c6fca1a3c650056521b01d15a72da`

Renamed WinRAR:

`d0c3d7003b7f5b4a3bd74a41709cfecfabea1f94b47e1162142de76aa7a063c7`

Renamed csvde:

`7d2780cd9acc516b6817e9a51b8e2889f2dec455295ac6e6d65a6191abadebff`

Network Indicators

POST requests sent to the following URLs:

`/RestAPI/ImportTechnicians?step=1`

Domains:

`seed.nkn[.]org`

Note: the domain seed.nkn[.]org is a New Kind of Network (NKN) domain that provides legitimate peer to peer networking services utilizing blockchain technology for decentralization. It is possible to have false positive hits in a corporate network environment and it should be considered suspicious to see any software-initiated contacts to this domain or any subdomain.

Log File Analysis

Check serverOut*.txt log files under C:\ManageEngine\ServiceDesk\logs\ for suspicious log entries matching the following format:

```
[<time>]|[<date>]|
[com.adventnet.servicedesk.setup.action.ImportTechniciansAction]|
[INFO]|[62]: fileName is : msiexec.exe]
```

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

Tactics, Techniques, and Procedures

- Using WMI for lateral movement and remote code execution (in particular, `wmic.exe`)
- Using plaintext credentials for lateral movement
- Using `pg_dump.exe` to dump ManageEngine databases
- Dumping `NTDS.dit` and `SECURITY/SYSTEM/NTUSER` registry hives
- Active credential harvesting through `LSASS` (KDC Sponge)
- Exfiltrating through webshells
- Conducting exploitation activity often through other compromised U.S. infrastructure
- Dropping multiple webshells and/or implants to maintain persistence
- Using renamed versions of `WinRAR`, `csvde`, and other legitimate third-party tools for reconnaissance and exfiltration

Yara Rules

```
rule ReportGenerate_jsp {
  strings:
    $s1 = "decrypt(fpath)"
    $s2 = "decrypt(fcontext)"
    $s3 = "decrypt(commandEnc)"
    $s4 = "upload failed!"
    $s5 = "sevck"
    $s6 = "newid"
  condition:
    filesize < 15KB and 4 of them
}

rule EncryptJSP {
  strings:
    $s1 = "AEScrypt"
    $s2 = "AES/CBC/PKCS5Padding"
    $s3 = "SecretKeySpec"
    $s4 = "FileOutputStream"
    $s5 = "getParameter"
    $s6 = "new ProcessBuilder"
    $s7 = "new BufferedReader"
    $s8 = "readLine()"
  condition:
    filesize < 15KB and 6 of them
}

rule ZimbraImplant {
   strings:
      $u1 = "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

```
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36"
        $u2 = "Content-Type: application/soap+xml; charset=UTF-8"
        $u3 = "/service/soap"
        $u4 = "Good Luck :::)"
        $s1 = "zimBR"
        $s2 = "log10"
        $s3 = "mymain"
        $s4 = "urn:zimbraAccount"
        $s5 = "/service/upload?fmt=extended,raw"
        $s6 = "<query>(in:\"inbox\" or in:\"junk\") is:unread</query>"
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 2MB and
1 of ($u*) and 3 of ($s*)
}

rule GodzillaDropper {
    strings:
        $s1 = "UEsDBAoAAAAAAI8UXFM" // base64 encoded PK/ZIP header
        $s2 = "../lib/tomcat/tomcat-postgres.jar"
        $s3 = "RunAsManager.exe"
        $s4 = "ServiceDesk"
        $s5 = "C:\\Users\\pwn\\documents\\visual studio 2015\\Projects\\payloaddll"
        $s6 = "CreateMutexA"
        $s7 = "cplusplus_me"
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 350KB
and 4 of them
}

rule GodzillaJAR {
    strings:
        $s1 = "org/apache/tomcat/SSLFilter.class"
        $s2 = "META-INF/services/javax.servlet.ServletContainerInitializer"
        $s3 = "org/apache/tomcat/MainFilterInitializer.class"
    condition:
        uint32(0) == 0x04034B50 and filesize < 50KB and all of them
}

rule APT_NGLite {
    strings:
        $s1 = "/mnt/hgfs/CrossC2-2.2"
        $s2 = "WHATswrongwithU"
        $s3 = "//seed.nkn.org:"
```

```
        $s4 = "Preylistener"
        $s5 = "preyid"
        $s6 = "Www-Authenticate"
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 15MB
and 4 of them
}

rule KDCSponge {
    strings:
        $k1 = "kdcsvc.dll"
        $k2 = "kdccli.dll"
        $k3 = "kdcsvs.dll"
        $f1 = "KerbHashPasswordEx3"
        $f2 = "KerbFreeKey"
        $f3 = "KdcVerifyEncryptedTimeStamp"
        $s1 = "download//symbols//%S//%S//%S" wide
        $s2 = "KDC Service"
        $s3 = "\\system.dat"
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 1MB and
1 of ($k*) and 1 of ($f*) and 1 of ($s*)
```

Mitigations

Compromise Mitigations

Organizations that identify any activity related to ManageEngine ServiceDesk Plus indicators of compromise within their networks should take action immediately.

Zoho ManageEngine ServiceDesk Plus build 11306, or higher, fixes CVE-2021-44077. ManageEngine initially released a patch for this vulnerability on September 16, 2021. A subsequent security advisory was released on November 22, 2021, and advised customers to patch immediately. Additional information can be found in the Zoho security advisory released on November 22, 2021.

In addition, Zoho has set up a security response plan center that provides additional details, a downloadable tool that can be run on potentially affected systems, and a remediation guide.

FBI and CISA also strongly recommend domain-wide password resets and double Kerberos TGT password resets if any indication is found that the `NTDS.dit` file was compromised.

Note: Implementing these password resets should not be taken as a comprehensive mitigation in response to this threat; additional steps may be necessary to regain administrative control of your network. Refer to your specific products mitigation guidance for details.

Actions for Affected Organizations

Immediately report as an incident to CISA or the FBI (refer to Contact information section below) the existence of any of the following:

- Identification of indicators of compromise as outlined above.
- Presence of webshell code on compromised ServiceDesk Plus servers.
- Unauthorized access to or use of accounts.
- Evidence of lateral movement by malicious actors with access to compromised systems.
- Other indicators of unauthorized access or compromise.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office
- CISA (888-282-0870 or Central@cisa.dhs.gov).

Revisions

December 2, 2021: Initial version

December 6, 2021: STIX file added

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.