TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

17 DEC 2021

FLASH Number

AC-000159-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact FBI CyWatch immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email: cywatch@fbi.gov | Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

APT Actors Exploiting Newly-Identified Zero Day in ManageEngine Desktop Central

Summary

Since at least late October 2021, APT actors have been actively exploiting a zero-day, now identified as CVE-2021-44515, on ManageEngine Desktop Central servers. The APT actors were observed compromising Desktop Central servers, dropping a webshell that overrides a legitimate function of Desktop Central, downloading post-exploitation tools, enumerating domain users and groups, conducting network reconnaissance, attempting lateral movement and dumping credentials.

CVE-2021-44515, which Zoho rated critical, addresses an authentication bypass vulnerability in ManageEngine Desktop Central software that can allow an adversary to bypass authentication and execute arbitrary code on Desktop Central servers.

Zoho released a ManageEngine Desktop Central Security Advisory for the newly identified vulnerability CVE-2021-44515 on December 3, 2021:

https://www.manageengine.com/products/desktop-central/cve-2021-44515-authentication-bypass-filter-configuration.html

Zoho also provided the following vulnerable build numbers for ManageEngine Desktop Central customers:

For Enterprise Customers:
For builds 10.1.2127.17 and below, upgrade to 10.1.2127.18
For builds 10.1.2128.0 to 10.1.2137.2, upgrade to 10.1.2137.3

For MSP Customers:
For builds 10.1.2127.17 and below, upgrade to 10.1.2127.18
For builds 10.1.2128.0 to 10.1.2137.2, upgrade to 10.1.2137.3

Technical Details

Initial exploitation of a Desktop Central API URL allowed for an unauthenticated file upload of two different variants of webshells observed in this campaign with the filenames `emsaler.zip` (variant 1, late October 2021), `eco-inflect.jar` (variant 1, mid November 2021) and `aaa.zip` (variant 2, late November 2021).

The webshell overrides the legitimate Desktop Central API servlet endpoint, `/fos/statuscheck`, and filters inbound GET (webshell variant 2) or POST requests (webshell variant 1) to that URL path and executes commands as the SYSTEM user with elevated privileges if the inbound requests pass the filter check.

Initial reconnaissance and domain enumeration was conducted through the webshell. After initial reconnaissance, the actors use BITSAdmin to download a likely ShadowPad variant dropper with filename `mscoree.dll`, and a legitimate Microsoft AppLaunch binary, `iop.exe`. The dropper is sideloaded through AppLaunch execution, which creates a persistent service to execute the AppLaunch binary moving forward. Upon execution, the dropper creates an instance of `svchost` and injects code with RAT-like functionality that initiates a connection to a command and control server.

Follow-on intrusion activity is then conducted through the RAT, including attempted lateral movement to domain controllers and credential dumping techniques using

Mimikatz, `comsvcs.dll` LSASS process memory dumping, and a WDigest downgrade attack with subsequent LSASS dumping through `pwdump`.

The malicious samples were downloaded from likely compromised ManageEngine ADSelfService Plus servers.

Indicators

Log File Analysis

1. Search access log files located at `%DesktopCentralInstallRoot%\logs\access_logs\access*` for:
    a. POST requests to the following URL(s):
        i. `/STATE_ID/123/agentLogUploader`
    b. GET or POST requests to the following URL(s):
        i. `/fos/statuscheck`

2. Search serverout log files located at `%DesktopCentralInstallRoot%\logs\serverout\*` for log lines matching a format similar to the following:
    a. `[<time>]|[<date>]|[com.adventnet.sym.webclient.statusupdate.AgentLogUploadServlet]|[WARNING]|[<num>]|[<guid>]: absolute Dir ..\ds-logs\1\../../\lib |`
    b. `[<time>]|[<date>]|[com.adventnet.sym.webclient.statusupdate.AgentLogUploadServlet]|[WARNING]|[<num>]|[<guid>]: absolute File Name aaa.zip |`
        i. Also replace `aaa.zip` with `emsaler.zip`, `eco-inflect.jar` or remove it altogether to expand the search.

NOTE: The `/fos/statuscheck` API URL is a legitimate Desktop Central function, but based on analysis appears to be rarely used, and only expects communications from other internal Desktop Central servers. Any requests between late October 2021 and early December 2021, or those originating from external IP addresses, should be considered suspicious and investigated.

Hashes

```
febf7f32fed44a4a58a2e0ea402ea181a0e1a519ea41fab1d4ccfb097c8e538c
44937538ff3a4316d60f672b7cddc9ba02cea2b991e25fafdb8b947622c8fe03
```

e4297e74a59e1e9b125a0b7c0a0f34b1a22010086b302f88d25a5ce18b1b70d4

a9b6ef095e16373d914937377bebe78fa9ca319741a3c516c18171073336269e

f6223d956df81dcb6135c6ce00ee14d0efede9fb399b56d2ee95b7b0538fe12c

4fbc93dd537ca67c3aa0e9082dc5189f81968b26a0cc69f07424b47f27d52049

aaa77fffdb9f23ce13da059779cdb8df785e9f321bb2044be2213774e1af817

4aeefe0140d7ea0a7e90f1027957ad4f3ae171116e2a255bdcb2a16b74209249

ede143975a065c04baa7df73a991a59aa090ae0c49f9d0b920fa263086b5f676

1b80c6bf098be080c8275fe7d7234f2d34f50ed403541b9b60490ab2b704d4dd

18ebe6045bedc9ed7cff6e6aae4326b97699eb5bc71f8a514b9e13857edb6a9f

Services

Name: MicrosoftFrameworkLaunchUtility

Executable Path: C:\ProgramData\MicroSoft Framework\Microsoft.Framework.AppLaunch.exe

RAT Path: C:\ProgramData\MicroSoft Framework\mscoree.dll

Processes

svchost.exe running MicrosoftFrameworkLaunchUtility

Domains

ns2.latincop[.]com

Filepaths

\ManageEngine\DesktopCentral_Server\lib\aaa.zip

\ManageEngine\DesktopCentral_Server\lib\emsaler.zip

\ManageEngine\DesktopCentral_Server\lib\eco-inflect.jar

C:\windows\ime\ssp.dll

C:\windows\ime\iop.exe

C:\windows\ime\mscoree.dll

```
C:\ProgramData\MicroSoft
Framework\Microsoft.Framework.AppLaunch.exe

C:\ProgramData\MicroSoft Framework\mscoree.dll
```

Tactics, Techniques and Procedures

- DLL sideloading
- Executing “live off the land” tools, e.g. bitsadmin
- Network scanning, e.g. nbtscan, nb.exe
- Powershell for command execution
- Persistence through Windows Service
- Downloading staged post-exploitation tools from other victim infrastructure
- Credential dumping, e.g. Mimikatz, comsvcs.dll, WDigest downgrade and pwdump

Yara Rules

```
import "pe"

rule mscoree_RAT_loader_func {
    strings:
        $s1 = { FF 15 ?? AF 00 00 80 B8 04 41 00 00 48} //
GetModuleHandleA initial load
        $s2 = { 33 C9 BA A3 4F 01 00 } // size allocation: 85923
bytes, could vary
        $s3 = { 41 B8 00 10 00 00 44 8D 49 40 } // 0x40 RWX allocation
        $s4 = { FF 15 17 AF 00 00 }

    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)
and filesize < 350KB and 3 of them
}

rule mscoree_RAT {
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550)
        and filesize < 350KB
        and pe.dll_name == "MSCOREE.dll"
        and pe.exports("IEE")
        and pe.imports("kernel32.dll", "VirtualAlloc") and
pe.imports("kernel32.dll", "IsDebuggerPresent")
}

rule StatusCheck_backdoor_zip {
    strings:
        $s1 = "com/zoho/clustering/agent/api/StatusCheck.class"
        $s2 = "META-INF/MANIFEST.MF"

    condition:
        uint32(0) == 0x04034B50 and filesize < 15KB and all of them
}

rule aaa_fos_statuscheck_class {
    strings:
        $s1 = "decodeBase64"
        $s2 = "APIKEYS" fullword
        $s3 = "slaveId"
        $s4 = "processRequest"
        $s5 = "com/zoho/clustering/agent/remotemonitor/MonitorPool"
        $s6 = "destnAbsoluteFileName"
        $s7 = "Fail" fullword
        $s8 = "lognames" fullword
        $s9 = "receivedFileSize"
        $s10 = "<TITLE>ManageEngine Desktop Central</TITLE>"

    condition:
        uint32(0) == 0xbebafeca and filesize < 15KB and 7 of them
}

rule APT_backdoor_class {
    strings:
        $s1 = "cmd.exe /c"
        $s2 = "Authorization-Expires"
        $s3 = "encrypt"
        $s4 = "encodeBase64"
        $s5 = "prepareDownload"
        $s6 = "application/octet-stream;charset=UTF-8"
        $s7 = "getUploadedFile"
        $s8 = "Agent64Com"
        $s9 = "cmd_flag"
    condition:
        uint32(0) == 0xbebafeca and filesize < 15KB and 6 of them
}

rule APT_backdoor_RC4_class {
    strings:
        $s1 = "com/zoho/clustering/agent/api/RC4"
        $s2 = "StackMapTable"
        $s3 = "RC4.java"
        $s4 = "in_offset"
        $s5 = "out_offset"
        $s6 = "encrypt"

    condition:
        uint32(0) == 0xbebafeca and filesize < 5KB and 5 of them
}
```

Information Requested:

Please report to FBI the existence of any of the following:

- Identification of indicators of compromise (IOCs) as outlined above
- Presence of webshell code on compromised Desktop Central servers
- Unauthorized access to or use of accounts
- Evidence of lateral movement by malicious actors with access to compromised systems
- Malicious IPs identified through conducted log file searches and session activity
- Malicious samples identified through IOCs
- Other indicators of unauthorized access or compromise

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

Recommended Mitigations:

Organizations that identify any activity related to these IOCs within their networks should take action immediately.

Zoho released a ManageEngine Desktop Central Security Advisory for the newly identified vulnerability CVE-2021-44515 on December 3, 2021:

https://www.manageengine.com/products/desktop-central/cve-2021-44515-authentication-bypass-filter-configuration.html

Zoho also provided the following vulnerable build numbers for ManageEngine Desktop Central customers:

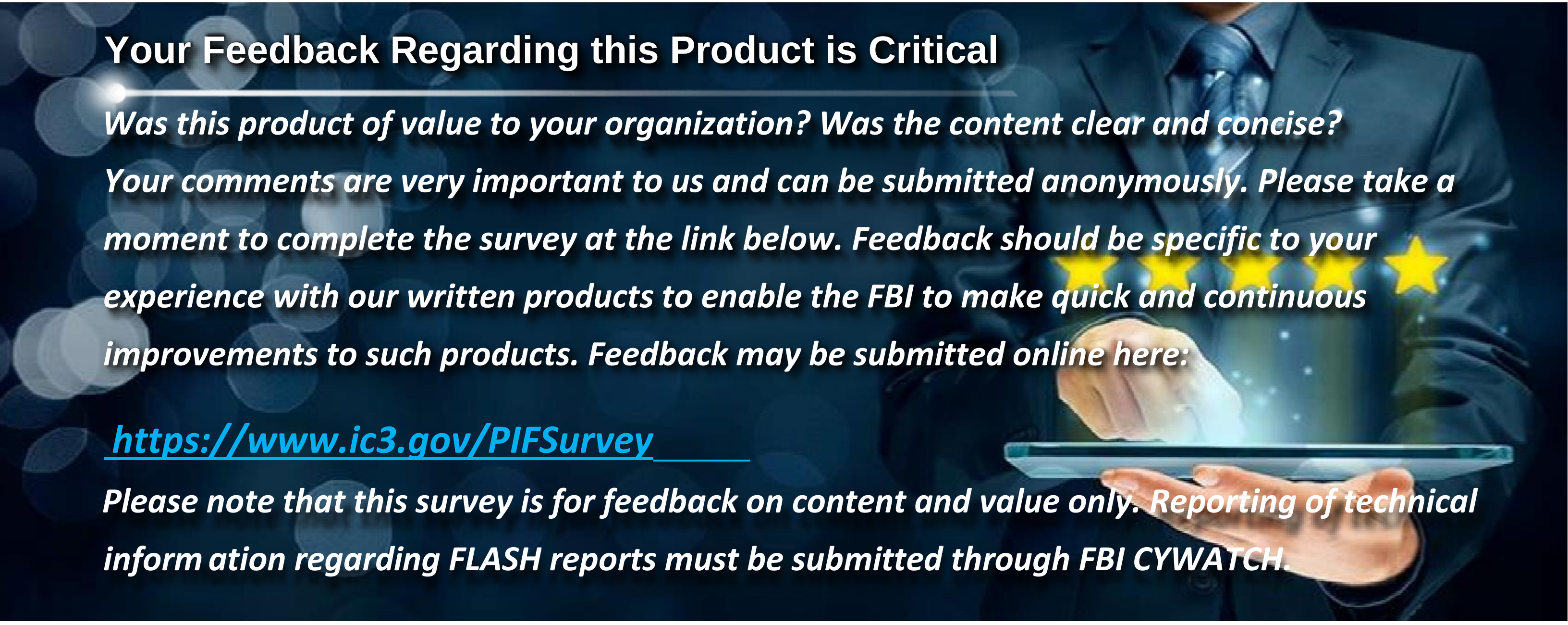
For Enterprise Customers:
For builds 10.1.2127.17 and below, upgrade to 10.1.2127.18
For builds 10.1.2128.0 to 10.1.2137.2, upgrade to 10.1.2137.3

For MSP Customers:
For builds 10.1.2127.17 and below, upgrade to 10.1.2127.18
For builds 10.1.2128.0 to 10.1.2137.2, upgrade to 10.1.2137.3

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.



Your Feedback Regarding this Product is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.