JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-069A

March 10, 2021

Compromise of Microsoft Exchange Server

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise framework for referenced threat actor techniques and for mitigations.

SUMMARY

This 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 vulnerabilities in Microsoft Exchange on-premises products. The FBI and CISA assess that nation-state actors and cyber criminals are likely among those exploiting these vulnerabilities. The exploitation of Microsoft Exchange on-premises products poses a serious risk to Federal Civilian Executive Branch agencies and private companies. Successful exploitation of these vulnerabilities allows an attacker to access victims' Exchange Servers, enabling them to gain persistent system access and control of an enterprise network. It has the potential to affect tens of thousands of systems in the United States and provides adversaries with access to networks containing valuable research, technology, personally identifiable information (PII), and other sensitive information from entities in multiple U.S. sectors. FBI and CISA assess that adversaries will continue to exploit this vulnerability to compromise networks and steal information, encrypt data for ransom, or even execute a destructive attack. Adversaries may also sell access to compromised networks on the dark web.

On March 2, 2021, Microsoft and Volexity announced the detection of multiple zero-day exploits used to target vulnerabilities in on-premises versions of Microsoft Exchange Servers. In light of this public announcement, FBI and CISA assess that other capable cyber actors are attempting to exploit these vulnerabilities before victims implement the Microsoft updates.

The FBI and CISA have reports of malicious cyber actors using zero-day exploits CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 to gain access [T1190] to on-premises Microsoft Exchange servers of U.S. entities as early as January 2021. Various Tactics, Techniques,

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

and Procedures (TTPs) have been identified, but the actor(s) frequently appeared to be writing webshells [T1505.003] to disk for initial persistence, conducting further operations to dump user credentials [T1003], adding/deleting user accounts as needed [T1136], stealing copies of the Active Directory database (`NTDS.dit`) [T1003.003], and moving laterally to other systems and environments. The actors appear to be collecting [T1114], compressing [T1560.001], and exfiltrating mailbox data. This information has been shared with multiple U.S. government (USG) agencies and partners.

The FBI is proactively investigating this malicious cyber activity, leveraging 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. 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 cyber activities.

See the CISA Remediating Microsoft Exchange Vulnerabilities web page for both executive- and technical-level guidance. Additionally, refer to the following CISA Alert for full technical details that address the four vulnerabilities in Microsoft Exchange Servers and associated IOCs.

- Alert (AA21-062A): Mitigate Microsoft Exchange Server Vulnerabilities

TECHNICAL DETAILS

On March 2, 2021, Microsoft released security updates for several zero-day exploits (CVE 2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065). Continual use of unpatched exchange servers or delayed implementation of Microsoft-released updates poses a serious risk to affected systems. It is highly likely that malicious cyber actors will continue to use the aforementioned exploits to target and compromise the networks of U.S. entities for cyber-enabled espionage, data exfiltration, and criminal activity.

Targeted Sectors

Threat actors have targeted local governments, academic institutions, non-governmental organizations, and business entities in multiple industry sectors, including agriculture, biotechnology, aerospace, defense, legal services, power utilities, and pharmaceutical. This targeting is consistent with previous targeting activity by Chinese cyber actors. Illicitly obtained business information, advanced technology, and research data may undermine business operations and research development of many U.S. companies and institutions.

Note: *the technical information below was partially derived from multiple open source reports. CISA and the FBI are republishing it, in part, to provide a consolidated guide and to highlight the importance of mitigating these vulnerabilities.*

Log File Analysis

Any file below the following file path can be targeted with `XML SOAP POST` requests for unauthenticated execution. Check log files for `POST` requests to these resources:

```
/owa/auth/Current/themes/resources/*
```

Example file paths targeted:

- `/owa/auth/Current/themes/resources/logon.css`
- `/owa/auth/Current/themes/resources/owafont_ja.css`
- `/owa/auth/Current/themes/resources/lgnbotl.gif`
- `/owa/auth/Current/themes/resources/owafont_ko.css`
- `/owa/auth/Current/themes/resources/SegoeUI-SemiBold.eot`
- `/owa/auth/Current/themes/resources/SegoeUI-SemiLight.ttf`
- `/owa/auth/Current/themes/resources/lgnbotl.gif`

Check Exchange ECP server logs for the following:

```
S:CMD=Set-OabVirtualDirectory.ExternalUrl=
```

Note: ECP Server logs are typically located at `<exchange install path>\Logging\ECP\Server\`.

Check IIS logs for access to the following resource (this resource can be used legitimately, but should be noted):

```
/ecp/DDI/DDIService.svc/SetObject
```

PowerShell Commands

Running the PowerShell commands below on an Exchange server can help detect evidence that the following CVE's may have been exploited:

Detect Possible CVE-2021-26855 Exploitation

```
Import-Csv -Path (Get-ChildItem -Recurse -Path
"$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter
'*.log').FullName | Where-Object {  $_.AuthenticatedUser -eq '' -and
$_.AnchorMailbox -like 'ServerInfo~*/*' } | select DateTime, AnchorMailbox
```

Detect Possible CVE-2021-26858 Exploitation

```
findstr /snip /c:"Download failed and temporary file"
"%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog\*.log"
```

Detect Possible CVE-2021-26857 Exploitation

```
Get-EventLog -LogName Application -Source "MSExchange Unified Messaging" -
EntryType Error | Where-Object { $_.Message -like "*System.InvalidCastException*"
}
```

Detect Possible CVE-2021-27065 Exploitation

```
Select-String -Path "$env:PROGRAMFILES\Microsoft\Exchange
Server\V15\Logging\ECP\Server\*.log" -Pattern 'Set-.+VirtualDirectory'
```

Note: additional advanced SIEM hunting queries are available in the Microsoft Blog: HAFNIUM targeting Exchange Servers with 0-day exploits to help identify initial exploitation.

TTPs Identified:

- `Webshells (ASPX and PHP)`
- `rundll32 C:\windows\system32\comsvcs.dll MiniDump lsass.dmp`
- `PsExec`
- `ProcDump`
- `WinRar Command Line Utility`
- `7zip`
- `PowerCat (Github)`
- `Nishang (Github)`
- Adding and using PowerShell Snap-Ins (`Add-PSSnapin`) to export mailboxes (`Get-MailboxExportRequest`)

Addition/Deletion of Domain User Accounts/Groups

The malicious cyber actor(s) exploit vulnerabilities CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 to target and gain initial access to on-premises Microsoft Exchange Servers [T1190]. Web shells [T1505.003] are being deployed on servers of targets to establish persistence in the victim's Exchange Servers. The actor(s) gain credentialed access by using `Procdump` to dump `LSASS` process memory, [T1003.001], adding/deleting user accounts [T1136], and stealing copies of Active Directory (`NTDS.dit`) [T1003.003]. Lateral movement in the network can be achieved though these accounts and the use of `PSExec` [S0029] to execute commands on remote systems [T1021.002]. `PowerShell` [T1059.001] is used in this intrusion activity in import tools [T1105] as well as conduct system/network enumeration like Remote System Discovery [T1018], System Information Discovery [T1082], System Service Discovery [T1007], Network Service Scanning [T1046], File and Directory Discovery [T1083]. The actor(s) collect [T1114] and compress [T1560.001] the mailbox data with `7Zip` or `WinRAR` before exfiltrating victim emails. Multiple C2 nodes are being used for different stages of the intrusion activity [T1104].

File path Indicators:

- \inetpub\wwwroot\aspnet_client\ (any .aspx file under this folder or sub folders)
- \inetpub\wwwroot\aspnet_client\system_web\ (any .aspx file under this folder or sub folders)
- \<exchange install path>\FrontEnd\HttpProxy\ecp\auth\ (any file besides TimeoutLogoff.aspx)
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\ (any file or modified file that is not part of a standard install)
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\Current\<any aspx file in this folder or subfolders>
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\<folder with version number>\<any aspx file in this folder or subfolders>

Note: also check for suspicious .zip, .rar, and .7z files in C:\ProgramData\, which may indicate possible data exfiltration.

Filename Indicators (including, but not limited to):

- App_Web_<RANDOM.dll
- <RANDOM 8 Alphanum>.aspx
- web.aspx
- help.aspx
- document.aspx
- errorEE.aspx
- errorEEE.aspx
- errorEW.aspx
- errorFF.aspx
- healthcheck.aspx
- aspnet_www.aspx
- aspnet_client.aspx
- xx.aspx
- shell.aspx
- shellex.aspx

- aspnet_iisstart.aspx
- iistart.aspx
- one.aspx
- errorcheck.aspx
- t.aspx
- aspnettest.aspx
- error.aspx
- discover.aspx

Note: Any `.aspx` file that belongs to the `SYSTEM` account warrants additional investigation.

User Agent Strings (related to POST requests for files under /owa/auth/Current):

- DuckDuckBot/1.0;+(+http://duckduckgo.com/duckduckbot.html)
- facebookexternalhit/1.1+(+http://www.facebook.com/externalhit_uatext.php)
- Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
- Mozilla/5.0+(compatible;+Bingbot/2.0;++http://www.bing.com/bingbot.htm)
- Mozilla/5.0+(compatible;+Googlebot/2.1;++http://www.google.com/bot.html
- Mozilla/5.0+(compatible;+Konqueror/3.5;+Linux)+KHTML/3.5.5+(like+Gecko)+(Exabot-Thumbnails)
- Mozilla/5.0+(compatible;+Yahoo!+Slurp;+http://help.yahoo.com/help/us/ysearch/slurp)
- Mozilla/5.0+(compatible;+YandexBot/3.0;++http://yandex.com/bots)
- Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/51.0.2704.103+Safari/537.36

Note: These *can* have false positives but are non-standard user agent strings.

User Agent Strings (related to exploitation activity to /ecp/ URLs)

- ExchangeServicesClient/0.0.0.0
- python-requests/2.19.1
- python-requests/2.25.1

User Agent Strings (related to webshell post exploitation activity)

- antSword/v2.1

- Googlebot/2.1+(+http://www.googlebot.com/bot.html)
- Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)

Yara Rules

```
rule webshell_aspx_simpleseesharp : Webshell Unclassified {
    meta:
        author= "threatintel@volexity.com"
        date= "2021-03-01"
        description= "A simple ASPX Webshell that allows an attacker to write
further files to disk."
        hash= "893cd3583b49cb706b3e55ecb2ed0757b977a21f5c72e041392d1256f31166e2"

    strings:
        $header= "<%@ Page Language=\"C#\" %>"
        $body= "<% HttpPostedFile thisFile =
Request.Files[0];thisFile.SaveAs(Path.Combine"

    condition:
        $header at 0 and $body and filesize < 1KB
}

rule webshell_aspx_reGeorgTunnel : Webshell Commodity {
    meta:
        author= "threatintel@volexity.com"
        date= "2021-03-01"
        description= "variation on reGeorgtunnel"
        hash= "406b680edc9a1bb0e2c7c451c56904857848b5f15570401450b73b232ff38928"
        reference= "https://github.com/sensepost/reGeorg/blob/master/tunnel.aspx"

    strings:
        $s1= "System.Net.Sockets"
```

```
        $s2=
"System.Text.Encoding.Default.GetString(Convert.FromBase64String(StrTr(Request.He
aders.Get"
        $t1 = ".Split('|')"
        $t2= "Request.Headers.Get"
        $t3= ".Substring("
        $t4= "new Socket("
        $t5= "IPAddress ip;"

    condition:
        all of ($s*) or all of ($t*)
}

rule webshell_aspx_sportsball : Webshell {
    meta:
        author= "threatintel@volexity.com"
        date= "2021-03-01"
        description= "The SPORTSBALL webshell allows attackers to upload files or
execute commands on the system."
        hash= "2fa06333188795110bba14a482020699a96f76fb1ceb80cbfa2df9d3008b5b0a"

    strings:
        $uniq1= "HttpCookie newcook = new HttpCookie(\"fqrspt\",
HttpContext.Current.Request.Form"
        $uniq2= "ZN2aDAB4rXsszEvCLrzgcvQ4oi5J1TuiRULlQbYwldE="

        $var1= "Result.InnerText = string.Empty;"
        $var2= "newcook.Expires = DateTime.Now.AddDays("
        $var3= "System.Diagnostics.Process process = new
System.Diagnostics.Process()"
        $var4=
"process.StandardInput.WriteLine(HttpContext.Current.Request.Form[\""
```

```
        $var5= "else if
(!string.IsNullOrEmpty(HttpContext.Current.Request.Form[\""
        $var6= "<input type=\"submit\" value=\"Upload\" />"


    condition:
    any of ($uniq*) or all of ($var*)
}
```

ATT&CK PROFILE

Figure 1 and Table 1 provide summaries of the MITRE ATT&CK techniques observed.

Figure 1: MITRE ATT&CK enterprise techniques observed

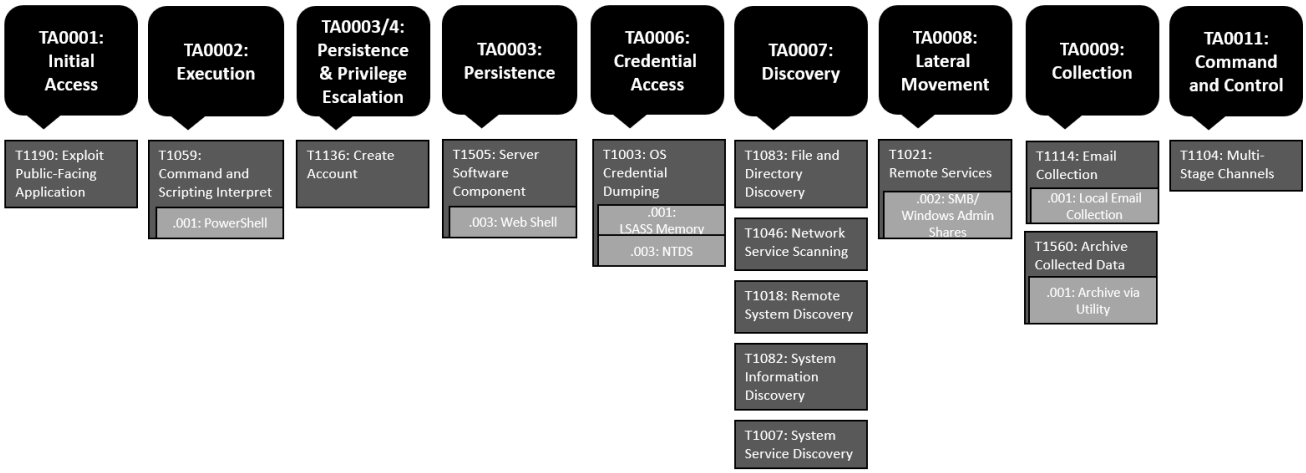

Table 1: MITRE ATT&CK techniques observed

Tactic Title	Technique ID	Technique Title
Initial Access [TA0001]	T1190	Exploit Public-Facing Application
Execution [TA0002]	T1059.001	Command and Scripting Interpreter: PowerShell

Persistence [TA0003] & Privilege Escalation [TA0004]	T1136.001	Create Account: Local Account
Persistence [TA0003]	T1505.003	Server Software Component: Web shell
Credential Access [TA0006]	T1003.001	OS Credential Dumping: LSASS Memory
	T1003.003	OS Credential Dumping: NTDS
Discovery [TA0007]	T1083	File and Directory Discovery
	T1046	Network Service Scanning
	T1018	Remote System Discovery
	T1082	System Information Discovery
	T1003	System Service Discovery
Lateral Movement [TA0008]	T1021.002	Remote Services: SMB/Windows Admin Shares
Collection [TA0009]	T1114.001	Email Collection: Local Email Collection
	T1560.001	Archive Collected Data: Archive via Utility
Command and Control [TA0011]	T1104	Multi-Stage Channels

MITIGATIONS

Compromise Mitigations

Organizations that identify any activity related to Microsoft Exchange Server indicators of compromise (IOCs) within their networks should take action immediately by following the process below:

1. After identifying all instances of on-premises Microsoft Exchange Servers in the environment, organizations that have the expertise should forensically triage artifacts using collection tools (see CISA's Activity Alert) to collect system memory, system web logs, windows event logs, and all registry hives. Organizations should then examine the artifacts for IOCs or anomalous behavior, such as credential dumping and other activities as described in the Alert. If there is anomalous behavior or an IOC detected, proceed to Action 2.

   If no IOCs have been found, organizations should immediately apply Microsoft patches for Microsoft Exchange servers and proceed to Action 5.

   If an organization does not have the expertise to forensically triage its systems, it should proceed to Action 3.

2. Organizations that have the expertise to take the following steps should do so before proceeding to Action 3. Organizations should examine artifacts collected in this step for IOCs or anomalous behavior, such as credential dumping, lateral movement, persistence mechanisms and other follow-on exploitation activity. Organizations without this expertise should proceed to Action 3.

    a. Forensically image system memory or, for virtual hosts, make a copy of the Virtual Memory (VMEM) to external storage for analysis.

    b. If a live forensic disk image can be acquired, follow your organization's procedures to acquire the live system disk image.

    c. If a live forensic disk image cannot be acquired, pause all instances of systems (virtual machines) running Outlook on the Web a.k.a. Outlook Web Access/App (collectively OWA) or Exchange Control Panel (ECP).

    d. Conduct forensic analysis of the system memory and disk image to look for IOCs provided in CISA Alert.

    e. Analyze stored network traffic and metadata for indications of compromise provided in CISA Alert or suspicious connections.

    f. Hunt the network and systems for additional indications of compromise, which will be provided in CISA Alert.

3. Organizations who have identified indications of compromise in Action 1, or did not have the expertise to conduct Action 1 or 2, should follow these steps and proceed to Action 4:

    a. Immediately disconnect Microsoft Exchange on-premises servers.

    b. Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.

4. CISA and FBI recommend you immediately report the existence of any of the following to CISA or the FBI:

    a. Identification of indicators of compromise as outlined in CISA Alert.

    b. Presence of web shell code on a compromised Microsoft Exchange on-premises server.

    c. Unauthorized access to or use of accounts.

    d. Evidence of lateral movement by malicious actors with access to compromised systems.

    e. Other indicators of unauthorized access or compromise.

    f. Other indicators related to this issue to be shared by CISA in the Alert.

Table 2: MITRE ATT&CK mitigations based on observed techniques

Mitigation	Description
User Training [M1017]	Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.
Privileged Process Integrity [M1025]	On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.
Privileged Account Management [M1026]	Limit the usage of local administrator accounts to be used for day-to-day operations that may expose them to potential adversaries.
	Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.
	Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.
	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.
Password Policies [M1027]	Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed.
	Ensure that local administrator accounts have complex, unique passwords across all systems on the network.
Operating System Configuration [M1028]	Consider disabling or restricting NTLM. Consider disabling WDigest authentication.

Multi-factor Authentication [M1032]	Use multi-factor authentication for user and privileged accounts.
Limit Access to Resource Over Network [M1035]	Consider disabling Windows administrative shares.
Filter Network Traffic [M1037]	Consider using the host firewall to restrict file sharing communications such as SMB.
Encrypt Sensitive Information [M1041]	Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.
	Ensure Domain Controller backups are properly secured.
Disable or Remove Feature or Program [M1042]	It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.
Credential Access Protection [M1043]	With Windows 10, Microsoft Implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware systems requirements. It also does not protect against all forms of credential dumping.
Code Signing [M1045]	Set PowerShell execution policy to execute only signed scripts.
Antivirus/Antimalware [M1049]	Anti-virus can be used to automatically quarantine suspicious files.

REFERENCES

- CISA Remediating Microsoft Exchange Vulnerabilities web page
- CISA Activity Alert (AA21-062A): Mitigate Microsoft Exchange Server Vulnerabilities
- Microsoft Blog: HAFNIUM targeting Exchange Servers with 0-day exploits
- Volexity Blog: Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities
- Splunk Blog: Detecting HAFNIUM Exchange Server Zero-Day Activity in Splunk