CYBERSECURITY ADVISORY

# Mitigate Microsoft Exchange Server Vulnerabilities

**Last Revised:** July 19, 2021 **Alert Code:** AA21-062A



## Summary

*Updated July 19, 2021: The U.S. Government attributes this activity to malicious cyber actors affiliated with the People's Republic of China (PRC) Ministry of State Security (MSS). Additional information may be found in a statement from the White House. For more information on Chinese malicious cyber activity, refer to us-cert.cisa.gov/China* <https://us-cert.cisa.gov/china>*.*

***Note:** This Alert was updated April 13, 2021, to provide further guidance.*

Cybersecurity and Infrastructure Security Agency (CISA) partners have observed active exploitation of vulnerabilities in Microsoft Exchange Server products. Successful exploitation of these vulnerabilities allows an unauthenticated attacker to execute arbitrary code on vulnerable Exchange Servers, enabling the attacker to gain persistent system access, as well as access to files and mailboxes on the server and to credentials stored on that system. Successful exploitation may additionally enable the attacker to compromise trust and identity in a vulnerable network. Microsoft released out-of-band patches to address vulnerabilities in Microsoft Exchange Server. The vulnerabilities impact on-premises Microsoft Exchange Servers and are not known to impact Exchange Online or Microsoft 365 (formerly O365) cloud email services.

This Alert includes both tactics, techniques and procedures (TTPs) and the indicators of compromise (IOCs) associated with this malicious activity. To secure against this threat, CISA recommends organizations examine their systems for the TTPs and use the IOCs to detect any malicious activity. If an organization discovers exploitation activity, they should assume network identity compromise and follow incident response procedures. If an organization finds no activity, they should apply available patches immediately and implement the mitigations in this Alert.

Click here for IOCs in STIX format. </sites/default/files/publications/aa21-062a.stix.xml>



## Technical Details

*(Updated April 14, 2021)*: Microsoft's April 2021 Security Update <https://msrc.microsoft.com/update-guide/releasenote/2021-apr> newly discloses and mitigates significant vulnerabilities affecting on-premises Exchange Server 2013, 2016, and 2019.

Microsoft has released out-of-band security updates to address four vulnerabilities in Exchange Server:

- CVE-2021-26855 allows an unauthenticated attacker to send arbitrary HTTP requests and authenticate as the Exchange Server. The vulnerability exploits the Exchange Control Panel (ECP) via a Server-Side Request Forgery (SSRF). This would also allow the attacker to gain access to mailboxes and read sensitive information.
- CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 allow for remote code execution.
  - CVE-2021-26858 and CVE-2021-27065 are similar post-authentication arbitrary write file vulnerabilities in Exchange. An attacker, authenticated either by using CVE-2021-26855 or via stolen admin credentials, could write a file to any path on the server.
  - CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service. An attacker, authenticated either by using CVE-2021-26855 or via stolen admin credentials, could execute arbitrary code as `SYSTEM` on the Exchange Server.
- To locate a possible compromise of these CVEs, CISA encourages organizations read the Microsoft Advisory.

It is possible for an attacker, once authenticated to the Exchange server, to gain access to the Active Directory environment and download the Active Directory Database.

*(Updated March 12, 2021):* Microsoft Security Intelligence has released a tweet <https://twitter.com/msftsecintel/status/1370236539427459076> on DearCry <https://www.bleepingcomputer.com/news/security/ransomware-now-attacks-microsoft-exchange-servers-with-proxylogon-exploits/> ransomware being used to exploit compromised on-premises Exchange Servers. Ransomware infections can have negative consequences to an affected organization, including:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

(*Updated April 12, 2021*): CISA recommends organizations review Malware Analysis Report (MAR) MAR-10330097-1.v1 – DearCry Ransomware <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-102b> for detailed analysis, along with TTPs and IOCs.

*(Updated March 12, 2021):* CISA encourages organizations to review CISA's Ransomware web page <https://www.cisa.gov/ransomware> for guidance and resources. Victims of ransomware should report it immediately to CISA at www.us-cert.gov/report <https://www.us-cert.gov/report>, a local FBI Field Office <https://www.fbi.gov/contact-us/field-offices>, or Secret Service Field Office <http://www.secretservice.gov/contact/field-offices/>.

## Tactics, Techniques and Procedures

*(Updated March 10, 2021):* Microsoft has released a script that scans Exchange log files for IOCs. CISA strongly encourages organizations to run the Test-ProxyLogon.ps1 script <https://github.com/microsoft/css-exchange/tree/main/security>—as soon as possible—to help determine whether their systems are compromised.

*(Updated March 16, 2021):* **Note:** Microsoft has released the Exchange On-premises Mitigation Tool (EOMT.ps1) <https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/> that can automate portions of both the detection and patching process. Microsoft stated the following along with the release: "[the tool is intended] to help customers who do not have dedicated security or IT teams to apply these security updates. We have tested this tool across Exchange Server 2013, 2016, and 2019 deployments. This new tool is designed as an interim mitigation for customers who are unfamiliar with the patch/update process or who have not yet applied the on-premises Exchange security update." Review the EOMT.ps1 blog post <https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/> for directions on using the tool.

*(Updated March 10, 2021):* CISA recommends investigating for signs of a compromise from at least January 1, 2021 through present.

*(Updated April 12, 2021):* CISA has identified 10 webshells associated with this activity. This is not an all-inclusive list of webshells that are being leveraged by actors. CISA recommends organizations review the following MARs for detailed analysis of the 10 webshells, along with TTPs and IOCs. These MARs include CISA-developed YARA rules to help network defenders detect associated malware.

1. AR21-072A: MAR-10328877.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072a>
2. AR21-072B: MAR-10328923.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072b>
3. AR21-072C: MAR-10329107.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072c>
4. AR21-072D: MAR-10329297.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072d>
5. AR21-072E: MAR-10329298.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072e>
6. AR21-072F: MAR-10329301.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072f>
7. AR21-072G: MAR-10329494.r1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072g>
8. AR21-084A: MAR-10329496-1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-084a>
9. AR21-084B: MAR-10329499-1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-084b>
10. AR21-102A: MAR-10331466-1.v1: China Chopper Webshell <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-102a>

*(Updated March 13, 2021):* A webshell is a script that can be uploaded to a compromised Microsoft Exchange Server to enable remote administration of the machine. Webshells are utilized for the following purposes:

- To harvest and exfiltrate sensitive data and credentials;

- To upload additional malware for the potential of creating, for example, a watering hole for infection and scanning of further victims;
- To use as a relay point to issue commands to hosts inside the network without direct internet access;
- To use as command-and-control infrastructure, potentially in the form of a bot in a botnet or in support of compromises to additional external networks. This could occur if the adversary intends to maintain long-term persistence.

*(Updated March 13, 2021):* For more information, see TA15-314A Compromised Web Servers and Web Shells - Threat Awareness and Guidance <https://us-cert.cisa.gov/ncas/alerts/ta15-314a>.

The majority of the TTPs in this section are sourced from a blog post from Volexity <https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/>, a third-party cybersecurity firm. **Note:** the United States Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government.

Volexity has observed the following files as targets of `HTTP POST` requests:

- `/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`

Administrators should search the ECP server logs for the following string (or something similar):

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

The logs can be found at `<exchange install path>\Logging\ECP\Server\`.

To determine possible webshell activity, administrators should search for `aspx` files in the following paths:

- `\inetpub\wwwroot\aspnet_client\` (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)

Administrators should search in the `/owa/auth/Current` directory for the following non-standard web log user-agents. These agents may be useful for incident responders to look at to determine if further investigation is necessary.



These should not be taken as definitive IOCs:

- `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`

Volexity observed these user-agents in conjunction with exploitation to `/ecp/` URLs:

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

These user-agents were also observed having connections to post-exploitation web-shell access:

- `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)`

As with the non-standard user-agents, responders can examine internet information services (IIS) logs from Exchange Servers to identify possible historical activity. Also, as with the non-standard user agents, these should not be taken as definitive IOCs:

- `POST /owa/auth/Current/`
- `POST /ecp/default.flt`

- `POST /ecp/main.css`
- `POST /ecp/<single char>.js`

Volexity has seen attackers leverage the following IP addresses. Although these are tied to virtual private servers (VPSs) servers and virtual private networks (VPNs), responders should investigate these IP addresses on their networks and act accordingly:

- `103.77.192[.]219`
- `104.140.114[.]110`
- `104.250.191[.]110`
- `108.61.246[.]56`
- `149.28.14[.]163`
- `157.230.221[.]198`
- `167.99.168[.]251`
- `185.250.151[.]72`
- `192.81.208[.]169`
- `203.160.69[.]66`
- `211.56.98[.]146`
- `5.254.43[.]18`
- `5.2.69[.]14`
- `80.92.205[.]81`
- `91.192.103[.]43`

Volexity has also provided the following YARA signatures that can be run within your network to assist in finding signs of a compromise.

```
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 = "A variation on the reGeorg tunnel webshell"
    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.Headers.Get"
    // a bit more experimental
```

```
        $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 Unclassified
{
    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*)
}
```

A list of webshell hashes have also been provided by Microsoft:

- `b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0`
- `097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e`
- `2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1`
- `65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5`
- `511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1`
- `4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f1f8ea`
- `811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d`
- `1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944`

**Note:** this is not an all-inclusive list of indicators of compromise and threat actors have been known to use short-term leased IP addresses that change very frequently. Organizations that do not locate any of the IOCs in this Alert within your network traffic, may nevertheless have been compromised. CISA recommends following the guidance located in the Microsoft Advisory to check your servers for any signs of a compromise.

## Conduct Forensic Analysis

Should your organization see evidence of compromise, your incident response should begin with conducting forensic analysis to collect artifacts and perform triage. Please see the following list of recommendations on how to conduct forensic analysis using various tools.

Although the following free tools are not endorsed by the Federal Government, incident responders commonly use them to perform forensics.

While collecting artifacts to perform triage, use processes and tools that minimize the alteration of the data being collected and that minimize impact to the operating system itself.

Ideally, during data collection, store the data on removable/external media and, when possible, run the artifact collection tools from the same media.

Key artifacts for triage that should be collected:

- Memory
- All registry hives
- All windows event logs
- All web logs

Memory can be collected with a variety of open source tools (e.g., FTK Imager by AccessData, Ram Capture by Belkasoft).

Registry and Windows Event logs can be collected with a variety of open source tools as well (e.g., FTK_Imager, Kroll Artifact Parser And Extractor [KAPE]).

Web logs can also be collected with a variety of open source tools (e.g., FTK Imager).

# Windows Artifact Collection Guide

Execute the following steps in order.

**1) Download the latest FTK Imager** from https://accessdata.com/product-download/ <https://accessdata.com/product-download/>.

- **Note:** Ensure your review of and compliance with the applicable license associated with the product referenced, which can be found in the product's User Guide. The United States Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government.

**2) Collect memory from live system using FTK Imager.** See Memory Capture with FTK Imager.pdf for instructions. Note: Download and copy "FTK Imager" folder to an external drive. Run FTK Imager.exe from the FTK Imager folder from external drive. Wait until memory collect is complete before proceeding to step 2.

**3) Collect important system artifacts using KAPE.** See KAPE Collection Procedure. Note: Download KAPE from a separate system; do not download KAPE to the target system. Run KAPE from external drive.

**4) Collect disk image using FTK Imager.** See Live Image with FTK Imager.pdf for instructions. **Note:** Run FTK Imager.exe from the "FTK Imager" folder from external drive.

# Memory Capture with FTK Imager

**1) Open FTK Imager.** Log into the system with Administrator privileges and launch "FTK Imager."

- **Note:** Ensure your review of and compliance with the applicable license associated with the product referenced. The United States Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government.

**2) Open "Capture Memory."** Select "Capture Memory…" from the File menu.

*Figure 1: FTK Imager – Capture Memory Command*

**3) Select Path and Filenames.** On the window that appears, use the "Browse" button to identify the destination of the memory capture. Save the memory capture to an external device and not the main hard drive of the system. Doing so will prevent the saved file from overwriting any dataspace on the system.

- Name the destination file with a descriptive name (i.e., hostname of the system).
- Select the box "Include pagefile" and provide a name of the pagefile that is descriptive of the system.
- Do not select "Create AD1 file."



*Figure 2: FTK Imager – Memory Capture*

**4) Capture Memory.** Click on "Capture Memory" to begin the capture process. The process will take several minutes depending on the size of the pagefile and the amount of memory on the system.

*Figure 3: FTK Imager – Capture Process*

## KAPE Collection Procedure [1 <https://ericzimmerman.github.io/kapedocs/#!pages%5c2.-getting-started.md>]

1) Download KAPE from https://www.kroll.com/en/services/cyber-risk/investigate-and-respond/kroll-artifact-parser-extractor-kape <https://www.kroll.com/en/services/cyber-risk/investigate-and-respond/kroll-artifact-parser-extractor-kape>.

2) Disable any antivirus or host protection mechanisms that prevent execution from removable media, or data loss prevention (DLP) mechanisms that restrict utilization of removable media.

- Enable antivirus and host protection once this process is completed.

3) Unzip Kape.zip and run gkape.exe as admin from your removable media

4) **Target source** should be the drive on which the OS resides, typically C:.

5) **Target destination** should be an external drive folder, not the same drive as the **Target source**. If available, use an external hard drive or flash drive.

- A KAPE execution with these parameters will typically produce output artifacts with a total size of 1-25 GB.
- If you are going to be running KAPE on different machines and want to save to the sam drive, ensure the Target destination folder is unique for each execution of KAPE.

6) Uncheck **Flush** checkbox (it is checked natively).

7) Check **Add %d** and **Add %m** checkboxes.

8) Select ALL checkboxes to ensure KAPE will target all available data that it is capable of targeting. This takes some time; use the down arrow and space bar to move through the list quickly.

9) Check **Process VSCs** checkbox.

10) Select **Zip** radio button and add Base name TargetOutput.

11) Ensure **Deduplicate** checkbox is checked (it is checked natively).

- At the bottom you should now see a large Current command line, similar to:

.\kape.exe --tsource C: --tdest E:\%d%m --tflush --target !BasicCollection,!SANS_Triage,Avast,AviraAVLogs,Bitdefender,ComboFix,ESET,FSecure,HitmanPro,Malwarebytes, McAfee,McAfee_ePO,RogueKiller,SentinelOne,Sophos,SUPERAntiSpyware,Symantec_AV_Logs,TrendMicro,VIPRE, Webroot,WindowsDefender,Ammyy,AsperaConnect,BoxDrive,CiscoJabber,CloudStorage,ConfluenceLogs,Discord, Dropbox, Exchange,ExchangeClientAccess,ExchangeTransport,FileZilla,GoogleDrive,iTunesBackup,JavaWebCache,Kaseya,LogMeIn,Notepad++, OneDrive,OutlookPSTOST,ScreenConnect,Skype,TeamViewerLogs,TeraCopy,VNCLogs, Chrome,ChromeExtensions,Edge,Firefox,InternetExplorer,WebBrowsers,ApacheAccessLog,IISLogFiles,ManageEngineLogs, MSSQLErrorLog,NGINXLogs,PowerShellConsole,KapeTriage,MiniTimelineCollection,RemoteAdmin, VirtualDisks, Gigatribe,TorrentClients,Torrents,$Boot,$J,$LogFile,$MFT,$SDS,$T,Amcache,ApplicationEvents,BCD,CombinedLogs, EncapsulationLogging,EventLogs,EventLogs-RDP,EventTraceLog EvidenceOfExecution,FileSystem,GroupPolicy,LinuxOnWindowsProfileFiles,LnkFilesAndJ mpLists,LogFiles,MemoryFiles, MOF,OfficeAutosave,OfficeDocumentCache,Prefetch,RDPCache,RDPLogs,RecentFileCache, Recycle, RecycleBin, RecycleBinContent,RecycleBinMetadata,RegistryHives,RegistryHivesSystem,RegistryHivesUser,ScheduledTasks,SDB, SignatureCatalog,SRUM,StartupInfo,Syscache,ThumbCache,USBDevicesLogs,WBEM,WER,WindowsFirewall, WindowsIndexSearch,WindowsNotifcationsDB,WindowsTimeline,XPRestorePoints --vss --zip TargetOutput –gui

- In the bottom right corner hit the **Execute!** Button.

- Screenshot below shows `gkape.exe` during execution, you will also see a command window execute. **Note:** KAPE usually takes less than 20 minutes to complete on a workstation; if it is taking significantly longer there may be an issue.

*Figure 4: gkape.exe screenshot*

## Mitigations

CISA strongly recommends organizations read Microsoft's advisory <https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/> and security blog post for more information on how to look for this malicious activity and to apply critical patches as soon as possible.

*(Updated March 4, 2021):* CISA is aware of threat actors using open source tools to search for vulnerable Microsoft Exchange Servers. This particular type of attack is scriptable, allowing attackers to easily exploit vulnerabilities through automated mechanisms. CISA advises all entities to patch as soon as possible to avoid being compromised.

*(Updated March 4, 2021):* From Microsoft's patch release <https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901>, the security updates are available for the following operating systems:

- Exchange Server 2010 (update requires SP 3 or any SP 3 RU – this is a Defense in Depth update)
- Exchange Server 2013 (update requires CU 23)
- Exchange Server 2016 (update requires CU 19 or CU 18)
- Exchange Server 2019 (update requires CU 8 or CU 7)

*(Updated March 4, 2021):* If you are running an older CU then what the patch will accept, you must upgrade to at least the required CU as stated above then apply the patch.

*(Updated March 4, 2021):* All patches must be applied using administrator privileges.

*(Updated March 5, 2021)*: If patching is not an immediate option, CISA strongly recommends following alternative mitigations found in Microsoft's blog on Exchange Server Vulnerabilities Mitigations <https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/>. However, these options should only be used as a temporary solution, not a replacement for patching. Additionally, there are other mitigation options available. CISA recommends limiting or blocking external access to internet-facing Exchange Servers via the following:

- Restrict untrusted connections to port 443, or set up a VPN to separate the Exchange Server from external access; note that this will not prevent an adversary from exploiting the vulnerability if the attacker is already in your network.
- Block external access to on-premises Exchange:
  - Restrict external access to OWA URL: `/owa/`.
  - Restrict external access to Exchange Admin Center (EAC) aka Exchange Control Panel (ECP) URL: `/ecp/`.
- *(Updated March 4, 2021):* Disconnect vulnerable Exchange servers from the internet until a patch can be applied.



CISA would like to thank Microsoft and Volexity for their contributions to this Alert.

## Resources

- (Updated April 14, 2021) **Microsoft's April 2021 Security Update** that mitigates significant vulnerabilities affecting on-premises Exchange Server 2013, 2016, and 2019.

- *(Updated March 12, 2021)* Check my OWA tool for checking if a system has been affected. ***Disclaimer:*** *this tool does not check against an exhaustive list of compromised domains. It is meant for informational purposes only. The United States Government does not provide any warranties of any kind regarding this information and cannot assure its accuracy or completeness; therefore, entities should not rely solely on this information to justify foregoing CISA's recommendations for action described on this webpage.*
- Microsoft Advisory: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/ <https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/>
- Microsoft Security Blog - Hafnium targeting Exchange Servers: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- Volexity Blog: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/ <//www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/>
- Microsoft's blog on Exchange Server Vulnerabilities Mitigations: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/ <https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/>

Give Feedback

## References


Eric Zimmerman: KAPE Documentation <https://ericzimmerman.github.io/kapedocs/#!pages%5c2.-getting-started.md>

Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities <https://cyber.dhs.gov/ed/21-02/>

Supplemental Direction V1 to Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities <https://cyber.dhs.gov/ed/21-02/#supplemental-direction>

Supplemental Direction V2 to Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities <https://cyber.dhs.gov/ed/21-02/#supplemental-direction-v2>

## Revisions

March 3, 2021: Initial Version|March 4, 2020: Updated Mitigations and Technical Details sections|March 5, 2021: Updated Mitigations Guidance from Microsoft|March 10, 2021: Updated TTP Section|March 12, 2021: Updated Resources Section|March 12, 2021: Added information on DearCry Ransomware |March 13, 2021: Added seven China Chopper Webshell MARs|March 14, 2021: Updated information on DearCry Ransomware|March 16, 2021: Added information on EOMT tool|March 25, 2021: Added two China Chopper Webshell MARs|March 25, 2021: Updated MARs to include YARA Rules|March 31, 2021: Added links to ED 21-02 and ED 21-02 Supplemental Direction|April 12, 2021: Added one China Chopper Webshell MAR and one DearCry Ransomware MAR|April 13, 2021: Added links to Microsoft's April 2021 Security Update and ED 21-02 Supplemental Direction V2|April 14, 2021: Added Exchange Server 2013 to list of on-premises Exchange Servers affected by the vulnerabilities dislcosed on April 13, 2021. |July 19, 2021: Added attribution note



## Tags

**Nation-State Actor**: China



Return to top




**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

**CISA Central**

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security