National Cyber Security Centre

21031001000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerabilities in Microsoft Exchange Servers - UPDATE2

(Indicators and Remediation for CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 & CVE-2021-27065)

2021-03-10

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Revision History

Revision	Date	Author(s)	Description
1.0	03 March 2021	CSIRT-IE	Initial Alert created regarding Microsoft Exchange Vulnerabilities
1.1	04 March 2021	CSIRT-IE	Additional information added regarding compromise of vulnerable servers prior to patching. TTPs section added with additional Indicators of Compromise and TTPs used by attackers
1.2	10 March 2021	CSIRT-IE	Additional information provided regarding actions required by organisations. Microsoft Exchange 2010 added to **Products Affected**. Mitre Att&ck techniques added to **Impact**. Additional information on web shells in **Threat Type**. Rapid7, Fireye, Palo Alto and Sophos advisories added to **Recommendations**, along with details on Microsoft scripts. Additional User-Agents, IP addresses and web shell cryptographic hashes added to **TTPs**

Threat Type

This updated Alert is being published in order to highlight to organisations the importance of carrying out investigative analysis to determine if Microsoft Exchange servers were compromised prior to patching the vulnerabilities below.

On 2nd March 2021, Microsoft released details of four vulnerabilities which are currently being exploited by attackers in Microsoft Exchange Servers. They have also released out-of-band Security Updates for Exchange Server to patch zero-day vulnerabilities

These vulnerabilities allow attackers to bypass authentication, including two-factor authentication, allowing them to access e-mail accounts of interest within targeted organisations and remotely execute code on vulnerable Microsoft Exchange servers.

- **CVE-2021-26855 (CVSS 3.0 9.1):** This vulnerability is a SSRF (Server Side Request Forgery) which allows an unauthenticated, remote attacker to exploit this flaw by sending a specially crafted HTTP request to a vulnerable Exchange Server. An attacker only requires the IP address or fully qualified domain name (FQDN) of an Exchange Server and the email account they wish to target in order to exfiltrate contents of a target mailbox.

- **CVE-2021-26857 (CVSS 3.0 7.8):** Is an insecure deserialization flaw in the Unified Messaging service; exploiting this allows attackers to run code as SYSTEM on the server

- **CVE-2021-26858 & CVE-2021-27065 (CVSS 3.0 7.8):** are both arbitrary file write vulnerabilities in Microsoft Exchange. These flaws are post-authentication, meaning an attacker would first need to authenticate to the vulnerable Exchange Server before they could exploit these vulnerabilities. These attacks have been observed being chained with CVE-2021-26855 or by possessing stolen administrator credentials. Once authenticated, an attacker could arbitrarily write to any paths on the vulnerable server.

UPDATE: Patching will provide protection from future exploitation of this vulnerability, however the NCSC advises that affected organisations **review the TTPs/ Recommendations section of this alert and search for any evidence of post-compromise activity on affected systems**.

It is important that organisations take urgent action regarding this issue.
If an organisation **has** the technical capability to follow the provided guidance, they should take those relevant steps.
If an organisation **does not have** the capability to follow the provided guidance, it is recommended that they seek assistance from a third-party IT security provider in order to ensure the security of their network.

Products Affected	• Microsoft Exchange Server 2010 **(CVE-2021-26857 only)** • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2019
Impact	Remote Code Execution, Email Collection, OS Credential Dumping, Exploit Public-Facing Application, Archive Collected Data, Acquire Infrastructure, Application Layer Protocol: Web Protocols, Exfiltration Over Web Service: Exfiltration to Cloud Storage, Create Account: Domain Account, Remote Services
Recommendations	Microsoft initially noted that these attacks were being exploited by a group they call **Hafnium**. However we understand that a number of other threat actor groups are now scanning for vulnerable services, exploiting them and deploying **web shells** on victims servers. A web shell is a post-exploitation tool that allows an attacker to maintain persistent access on a compromised web application. Web shells can be used to execute commands remotely, steal data, compromise server accounts or move laterally across a network. This allows attackers to deliver further malware payloads or exfiltrate sensitive data. The priority for organisations should be to apply the relevant patches as recommended by Microsoft. In conjunction with this, organisations **should investigate networks for exploitation or indicators of persistence**. NCSC-IE recommends the following action: • In order to investigate if you have already been compromised please refer to the Indicators of Compromise in the Microsoft Advisory • Read the Microsoft Blog post and apply the necessary updates and begin the investigative process as a matter of urgency • Microsoft has also published a related blog post regarding general practices around detection of malicious activity on your Exchange servers • Rapid7's Blog post provides technical analysis of this threat • Fireeye have provided details on the web shell activity, where they observed the process w3wp.exe, (the IIS process associated with the Exchange web front-end) spawning cmd.exe to write a file to disk • Florian Roth has created some YARA rules and Sigma Rules related to the advisories released by Microsoft and Volexity, which may help to detect suspicious activity on your Exchange servers • Palo Alto's Unit42 have detailed the role of one of the observed web shells being used in these attacks **China Chopper**

- Microsoft have provided the following scripts at their GitHub page, please ensure you read the instructions carefully before running any script on Exchange servers:
  - **Test-ProxyLogon.ps1:**This script automates all four of the commands found in the Hafnium blog post
  - **ExchangeMitigations.ps1:** This script contains 4 mitigations to help address vulnerabilities above, *This should only be used as a temporary mitigation until your Exchange Servers can be fully patched*
  - **CompareExchangeHashes.ps1:**This script provides a mechanism for malicious file detection on Exchange servers running Exchange2013, Exchange2016 or Exchange2019 versions
  - **BackendCookieMitigation.ps1:**This mitigation will filter https requests that contain malicious X-AnonResource-Backend and malformed X-BEResource cookies which were found to be used in CVE-2021-26855
  - **http-vuln-cve2021-26855.nse:**This file is for use with nmap. It detects whether the specified URL is vulnerable to the Exchange Server SSRF Vulnerability (CVE-2021-26855). For usage information, read the top of the file
- Sophos advises that if you are unable to patch, to implement an IIS Re-Write Rule and disable Unified Messaging (UM), Exchange Control Panel (ECP) VDir, and Offline Address Book (OAB) VDir Services.

TTPs

Volexity[1] and Dubex have been credited with reporting different parts of the attack chain and Volexity have published a blog post which outlines a number of the Tactics, Techniques and Procedures used by attackers.

HTTP POST requests were detected to the following files:

- /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

RCE appears to reside within the use of the Set-OabVirtualDirectory Exchange-PowerShell cmdlet. This activity can be found in the ECP Server logs (exchange install path \Logging\ECP\Server\.):

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

[1] https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

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 and CSIRT-IE have observed the following User-Agents in conjunction with exploitation to /ecp/ URLs.

```
ExchangeServicesClient/0.0.0.0
python-requests/2.19.1
python-requests/2.23.0
python-requests/2.24.0
python-requests/2.25.1
```

Further other notable User-Agent entries tied to tools used for post-exploitation access to webshells.

```
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)
```

A number of IP addresses used by attackers to exploit these vulnerabilities have been observed. Although these IP addresses are tied to VPS servers and VPN services, organisations should investigate evidence of these IP addresses on their network traffic (this is not an exhaustive list):

- 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
- 202[.]182.127.177
- 203[.]160.69.66
- 207[.]148.91.158
- 211[.]56.98.146
- 5[.]254.43.18
- 5[.]2.69.14
- 80[.]92.205.81
- 91[.]192.103.43
- 86.105.18.116
- 130.255.189.21
- 103.213.247.41
- 103.212.223.210

Webshell Hashes (sha256)

- b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
- 097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
- 2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
- 65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
- 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
- 4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
- 811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
- 1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie