National Cyber Security Centre

21030401000-NCSC

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

NCSC Flash Alert

Critical Vulnerabilities in Microsoft Exchange Servers - UPDATE

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

2021-03-04

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.*

Threat Type	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 section and search for any evidence of post-compromise activity on affected systems**. Please see the TTPs section below for referenced activity that may assist in your investigations
Products Affected	• Microsoft Exchange Server 2013 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2019
Impact	Remote Code Execution

Recommendations	Microsoft has noted that these attacks are currently being exploited by a group they call Hafnium, however it is expected that other groups will begin to exploit these vulnerabilities. NCSC-IE recommends the following action: • Review the Microsoft Blog post and apply the necessary updates or workarounds as a matter of urgency • There is an Exchange Server Health Checker script, which can be downloaded from GitHub (use the latest release). Running this script will tell you if you are behind on your on-premises Exchange Server updates (note that the script does not support Exchange Server 2010) • In order to investigate if you have already been compromised please refer to the Indicators of Compromise in the Microsoft Advisory • Microsoft has also published a related blog post regarding general practices around detection of malicious activity on your Exchange servers • 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
TTPs	Volexity 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=’

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 the following User-Agents in conjunction with exploitation to /ecp/ URLs.

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

Volexity observed numerous IP addresses used by attackers to exploit these vulnerabilities. Although these IP addresses are tied to VPS servers and VPN services, organisations should investigate evidence of these IP addresses on their network traffic:

- 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

TTP References:
Volexity - Operation Exchange Marauder
CISA Alert(AA21-062A)

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