Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP White

Advisory 2021-002: Active exploitation of vulnerable Microsoft Exchange servers

Document Version: 2, Last Updated: 18 March 2021

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has identified extensive targeting, and has confirmed compromises, of Australian organisations with vulnerable internet accessible Microsoft Exchange servers.

Summary

On 2nd March 2021 Microsoft released information regarding multiple exploits being used to compromise instances of Microsoft Exchange Server. Malicious actors are exploiting these vulnerabilities to compromise Microsoft Exchange servers exposed to the internet, enabling the malicious actor to access email accounts and to enable further compromise of the Exchange server and associated networks.

Information provided in this advisory should be used to shape and guide internal investigations and analysis in order to identify attempted exploitation of vulnerabilities or compromise of Microsoft Exchange Servers.

Vulnerability Details

There are four separate vulnerabilities which malicious actors are utilising to target exposed Microsoft Exchange servers.

- **CVE-2021-26855:** A server-side request forgery (SSRF) vulnerability in Exchange which allowed the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- **CVE-2021-26857:** An insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialised by a program. Exploiting this vulnerability gives an actor the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.
- **CVE-2021-26858:** A post-authentication arbitrary file write vulnerability in Exchange. If an actor could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.
- **CVE-2021-27065:** A post-authentication arbitrary file write vulnerability in Exchange. If an actor could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

Affected Microsoft Exchange versions

For the most accurate information on affected Microsoft Exchange versions please refer to guidance available from Microsoft[1]. At the current time the known vulnerable versions of Microsoft Exchange are:

- Microsoft Exchange 2010 (only vulnerable to CVE-2021-26857)
- Microsoft Exchange 2013

[1] Microsoft - Multiple Security Updates Released for Exchange Server

- Microsoft Exchange 2016
- Microsoft Exchange 2019

Exploitation and post-exploitation activities

The ACSC is aware of malicious actors exploiting CVE-2021-26855 for initial access to the vulnerable Microsoft Exchange servers. This vulnerability does not require authentication, and is trivial to exploit. Once initial exploitation is successful actors are able to retrieve e-mail inventories from all users stored on the server. In addition, malicious actors can exploit one of the other vulnerabilities to achieve arbitrary remote code execution or arbitrary file upload on the targeted server.

Malicious actors have leveraged these vulnerabilities to establish persistence utilising web shells on the compromised Microsoft Exchange servers, enabling further compromise of the Exchange server and associated internal network.

Mitigation and detection recommendations

ACSC recommended prioritised mitigations

The ACSC recommends immediate patching of all vulnerable Microsoft Exchange servers with Exchange servers exposed to the internet prioritised above servers accessible only on internal networks. All vulnerabilities identified in this advisory were patched by security updates released on 3 March 2021.

If patching is not possible immediately the following actions should be taken as soon as possible:

- Implement the interim mitigations advised by Microsoft[2], or
- Prevent access to vulnerable Microsoft Exchange servers from the internet, or
- Remove vulnerable Microsoft Exchange servers from the network.

These are temporary measures and only recommended where patching is not possible immediately.

Once patching or interim mitigations are applied the ACSC strongly recommends investigating all exposed Microsoft Exchange servers for signs of compromise.

ACSC recommended investigative actions

Regardless of how quickly patches were applied there remains a significant risk that malicious actors may have exploited and compromised vulnerable Microsoft Exchange servers prior to the application of patches. The following is a prioritised list of recommended investigative actions to check for signs of exploitation and compromise.

This guidance only covers looking for evidence of exploitation of the Microsoft Exchange vulnerabilities and web shell based post-exploitation activity. It is not intended as complete investigative guidance for all stages of an intrusion.

1. *Scan all Microsoft Exchange servers utilising the One-Click Microsoft Exchange On-Premises Mitigation Tool*

Microsoft have released the *One-Click Microsoft Exchange On-Premises Mitigation Tool* to help organisations implement interim mitigations as well as to scan and remove malicious files. Microsoft recommends running this tool on unpatched servers as well as servers which have been patched but not investigated for signs of exploitation and

[2] Microsoft – Microsoft Exchange Server Vulnerabilities Mitigations

compromise. Additionally Microsoft have identified that this tool replaces the previously released Microsoft mitigation script *ExchangeMitigations.ps1*. Details on the tool and future updates are available from Microsoft[3].

Microsoft has identified that this tool cannot be guaranteed to identify all malicious activity. The ACSC still recommends completing the additional investigative actions below.

2. *Review Microsoft Exchange log files for evidence of exploitation and compromise*

Microsoft has detailed which artifacts to review and what evidence to look for which can indicate exploitation for all four vulnerabilities. Microsoft have also release a PowerShell script to help organisations perform these checks. Details of the recommended analysis and the PowerShell script are available from Microsoft[4].

3. *Review file systems and HTTP log files for presence of known malicious web shell paths*

Web shells with identical filenames across multiple victims have been identified by multiple cyber security organisations. Organisations should review exposed Microsoft Exchange servers for the presence of these indicators and review any files for malicious content. The lack of any of these indicators above is not a guarantee of a lack of exploitation or successful compromise. Indicator sources include:

- Indicators from ACSC investigations available in **Appendix A – Indicators of compromise.**
- Identified host-based indicators of compromise available from Microsoft[5].
- Indicators of compromised references in the Cybersecurity and Infrastructure Security Agency's AA21-062A alert[6].

4. *Review and enact web shell identification and prevention guidance*

The Australian Signals Directorate and the National Security Agency collaborated to release some guidance on identifying and preventing web shells. It is recommended that organisations which had exposed Exchange servers review and act on this guidance. This guidance is available on cyber.gov.au[7].

Incident reporting

Organisations that have been impacted or have indications that your environment has been compromised can report a cyber security incident to the ACSC via cyber.gov.au[8].

[3] Microsoft – One-Click Microsoft Exchange On Premises Mitigation Tool
[4] Microsoft - HAFNIUM targeting Exchange Servers with 0-day exploits
[5] Microsoft HAFNIUM targeting Exchange Servers with 0-day exploits
[6] Cyber Security and Infrastructure Security Agency Alert AA21-062A
[7] Cyber.gov.au - Web shell malware
[8] Cyber.gov.au – ReportCyber

Appendix A: Indicators of compromise

In addition to some of the indicators of compromise identified in other reporting the ACSC has identified these additional indicators from ongoing ACSC investigations. Organisations are recommended to review these indicators as well as those identified by Microsoft and CISA in their respective guidance outlined previously in this advisory.

Indicator	Indicator type	MITRE ATT&CK	Description	Version added
error_page.aspx	File Name	T1505.003	Simple eval() web shell enabling arbitrary JScript code execution.	1
sol.aspx	File Name	T1505.003	Simple eval() web shell enabling arbitrary JScript code execution.	1
MultiUp.aspx	File Name	T1505.003	Web shell consisting only of file upload capability.	1

TLP: WHITE

Appendix B: MITRE ATT&CK Tactics and Techniques

The below tactics and techniques are associated with the initial exploitation of Microsoft Exchange servers and the common immediate post-exploitation activities. These tactics and techniques do not attempt to capture all possible actor tradecraft and actions resulting from exploitation of these vulnerabilities. The MITRE ATT&CK®[9] framework is used to capture these tactics and techniques.

Initial Access

T1190 – Exploit Public-Facing Application

Initial access is gained by malicious actors leveraging one or more of the CVE's identified in this advisory. Exploitation of CVE-2021-26855 is a requirement, unless the malicious actor already has privileged authenticated access to the Microsoft Exchange server.

Further information on the Exploit Public-Facing Application technique is available from MITRE[10].

Execution

T1203 – Exploitation for Client Execution

Exploitation of CVE-2021-26857 allows a malicious actor to execute arbitrary code with SYSTEM privileges on a vulnerable Microsoft Exchange server.

Further information on the Exploitation for Client Execution technique is available from MITRE[11].

Persistence

T1505.003 Server Software Component – Web Shell

Utilising CVE-2021-26857, CVE-2021-26858 or CVE-2021-27065 malicious actors can deploy web shells, amongst other tools, to enable persistence and execution on compromised Microsoft Exchange servers.

Further information on the Web Shell technique is available from MITRE[12].

Privilege Escalation

T1068 – Exploitation for Privilege Escalation

CVE-2021-26855 enables a malicious actor to achieve privilege escalation from an unauthenticated entity to a privileged user.

[9] MITRE ATT&CK

[10] MITRE ATT&CK Exploit Public-Facing Application

[11] MITRE ATT&CK Exploitation for Client Execution

[12] MITRE ATT&CK Web Shell

Further information on the Exploitation for Privilege Escalation technique is available from MITRE[13].

Collection

T1114.002 – Email Collection – Remote Email Collection

Successful exploitation of these vulnerabilities can allow a malicious actor to access user mailboxes on the compromised Microsoft Exchange server. It is possible that once additional malicious tools are deployed that a malicious actor could collect email through other means.

Further information on the Remote Email Collection technique is available from MITRE[14].

Command and Control

T1071.001 – Application Layer Protocol – Web Protocols

A standard technique due to the method of exploitation via HTTP, as well as HTTP-based communication with deployed web shells.

Further information on the Web Protocols technique is available from MITRE[15].

T1105 – Ingress Tool Transfer

The ACSC has identified the actor transferring malicious tools via command and control channels, both as a consequence of exploiting CVE-2021-26858 or CVE-2021-27065, as well as via a web shell whose sole purpose was to write an uploaded file to disk but had no native execution capabilities of its own.

Further information on the Ingress Tool Transfer technique is available from MITRE[16].

[13] MITRE ATT&CK Exploitation for Privilege Escalation

[14] MITRE ATT&CK Remote Email Collection

[15] MITRE ATT&CK Web Protocols

[16] MITRE ATT&CK Ingress Tool Transfer

TLP: WHITE

Traffic light protocol

TLP Level	Restriction on access and use
RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
AMBER	**Limited disclosure, restricted to participant's organisations..** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
WHITE	**Disclosure is not limited.** Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Not classified	Any information received from the ACSC that is not classified in accordance with the Traffic light protocol must be treated as AMBER classified unless otherwise agreed in writing by the ACSC.

TLP: WHITE

Document Change Log

Version	Change Summary
2	• Include reference to *Microsoft's One-Click Microsoft Exchange On-Premises Mitigation Tool*. • Reference Exchange 2010 vulnerability to CVE-2021-26857.
1	First published.