Emergency Directive 21-02

March 3, 2021

Mitigate Microsoft Exchange On-Premises Product Vulnerabilities

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 21-02, "*Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*".

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." *44 U.S.C. § 3553(h)(1)–(2)*

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. *6 U.S.C. § 655(3).*

Federal agencies are required to comply with these directives. *44 U.S.C. § 3554 (a)(1)(B)(v)*

These directives do not apply to statutorily-defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. *44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).*

Background

CISA partners have observed active exploitation of vulnerabilities in Microsoft Exchange *on-premises* products. *Neither the vulnerabilities nor the identified exploit activity is currently known to affect Microsoft 365 or Azure Cloud deployments.* Successful exploitation of these vulnerabilities allows an attacker to access on-premises Exchange Servers, enabling them to gain persistent system access and control of an enterprise network.

CISA has determined that this exploitation of Microsoft Exchange on-premises products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. This determination is based on the current exploitation of these vulnerabilities in the wild, the likelihood of the vulnerabilities being exploited, the prevalence of the affected software in the federal enterprise, the high potential for a compromise of agency information systems, and the potential impact of a successful compromise.

Currently, the vulnerabilities related to this known exploitation activity include CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065. According to Microsoft and security researchers, the following vulnerabilities are related yet not known to be exploited: CVE-2021-26412, CVE-2021-26854, CVE-2021-27078.

Required Actions

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

If no indications of compromise have been found, agencies must immediately apply Microsoft patches for Microsoft Exchange servers and proceed to Action 5.

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

---

2. Agencies that have the expertise to take the following steps immediately must do so before proceeding to Action 3. Agencies shall examine artifacts collected in this step for indications of compromise or anomalous behavior, such as credential dumping, lateral movement, persistence mechanisms and other follow on exploitation activity. Agencies without this expertise shall 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 Agency 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 Activity Alert

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

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

---

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

   a. Immediately disconnect Microsoft Exchange on-premises servers.

   b. Until such time as CISA directs these entities to rebuild the Microsoft Exchange Server operating system and reinstall the software package, agencies are prohibited from (re)joining the Microsoft Exchange Server to the enterprise domain.

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

   d. Affected entities should expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available.

---

4. Immediately report as an incident to CISA the existence of any of the following:

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

5. All agencies shall submit a report to CISA using the provided template by **noon Eastern Standard Time on Friday, March 5, 2021**. Department-level Chief Information Officers (CIOs) or equivalents must submit this report attesting agency status to CISA.

These Required Actions apply to agencies operating Microsoft Exchange Servers in any information system, including an information system used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information.

CISA Actions

- CISA will continue to work with our partners to monitor for active exploitation associated with these vulnerabilities.
- CISA will release additional indicators of compromise as they become available.

- CISA will provide technical assistance to agencies without internal capabilities to comply with this directive.
- CISA will provide additional guidance to agencies via the CISA website, through an emergency directive issuance coordination call, and through individual engagements upon request (via CyberDirectives@cisa.dhs.gov).
- By April 5, 2021, CISA will provide a report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) identifying cross-agency status and outstanding issues.

Duration

This Emergency Directive remains in effect until all agencies operating Microsoft Exchange servers have applied the available patch or the Directive is terminated through other appropriate action.

Additional Information

- General information, assistance, and reporting – CyberDirectives@cisa.dhs.gov
- Reporting indications of potential compromise – Central@cisa.dhs.gov