Mitigate Microsoft Exchange On-Premises Product Vulnerabilities

cisa.gov/ed2102

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.

CISA issued ED 21-02 requiring federal civilian departments and agencies running Microsoft Exchange on-premises products to update or disconnect the products from their networks until updated with the Microsoft patch.

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.

CISA published a Remediating Microsoft Exchange Vulnerabilities web page that strongly urges all organizations to immediately address the recent Microsoft Exchange Server product vulnerabilities. As exploitation of these vulnerabilities is widespread and indiscriminate, CISA strongly advises organizations follow the guidance laid out in the web page. The guidance provides specific steps for both leaders and IT security staff and is applicable for all sizes of organizations across all sectors.

Emergency Directive

CISA Updates the Supplemental Direction on Emergency Directive 21-02: On April 13, CISA updated the emergency directive for on-premises Microsoft Exchange servers and requires that agencies immediately apply the Microsoft April 2021 update to all affected Exchange Servers.

CISA Emergency Directive 21-02: CISA issued Emergency Directive (ED) 21-02 on March 3, requiring federal civilian departments and agencies running Microsoft Exchange on-premises products to update or disconnect the products from their networks until updated with the Microsoft patch.

Press Releases

CISA Issues Emergency Directive Requiring Federal Agencies to Patch Critical Vulnerability | CISA: On March 3, CISA issued a press release announcing the launch of Emergency Directive (ED) 21-02 requiring federal civilian departments and agencies running Microsoft Exchange on-premises products to update or disconnect the products from their networks until updated with the Microsoft patch.

Alerts and Guidance

MAR-10330097-1.v1: DearCry Ransomware identifies ransomware that has been used to exploit compromised on-premises Exchange servers. The malware encrypts files on a device and demands ransom in exchange for decryption.

MAR-10331466-1.v1: China Chopper Webshell identifies a China Chopper webshell observed in post-compromised Microsoft Exchange Servers. After successfully exploiting a Microsoft Exchange Server vulnerability for initial accesses, a malicious cyber actor can upload a webshell to enable remote administration of the affected system.

On March 31, CISA issued supplemental guidance to ED 21-02. The supplemental guidance provides additional forensic triage and server hardening requirements for federal agencies. Specifically, the supplemental direction requires agencies to run newly developed tools—Microsoft's Test-ProxyLogon.ps1 script and Safety Scanner (MSERT)—to investigate whether their Microsoft Exchange Servers have been compromised.

Updates on Microsoft Exchange Server Vulnerabilities: On March 13, CISA has added seven Malware Analysis Reports (MARs) to Alert AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities.

FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server: On March 10, CISA and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) to address recently disclosed vulnerabilities in Microsoft Exchange Server.

Mitigate Microsoft Exchange On-Premise Product Vulnerabilities: This document, published March 6, details actions needed to mitigate vulnerabilities addressed in ED- 2102.

Microsoft IOC Detection Tool for Exchange Server Vulnerabilities: Released March 6, This Current Activity Alert addresses a Microsoft released of [updated script] that scans Exchange log files for indicators of compromise (IOCs) associated with the [vulnerabilities] disclosed on March 2, 2021.

Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities: On March 5, CISA issued a Current Activity containing information on Microsoft's release of alternative mitigation techniques for Exchange Server customers who are not able to immediately apply updates that address vulnerabilities disclosed on March 2, 2021.

CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities | CISA: On March 3, CISA has issued Emergency Directive (ED) 21-02 and Alert AA21-062A addressing critical vulnerabilities in Microsoft Exchange products.

Mitigate Microsoft Exchange Server Vulnerabilities | CISA: On March 3, CISA issued an Activity Alert. This Alert includes both tactics, techniques and procedures (TTPs) and the indicators of compromise (IOCs) associated with this malicious activity. This Alert was updated on March 14 with seven Malware Analysis reports.

Microsoft Releases Out-of-Band Security Updates for Exchange Server | CISA: On March 2, CISA issued a Current Activity Alert with information related to Microsoft’s released out-of-band security updates to address vulnerabilities affecting Microsoft Exchange Server 2013, 2016, and 2019.