CyberSOC Threat Notification

Microsoft Exchange Server RCE Vulnerabilities

Executive Summary

On April 13th, 2021 Microsoft released four security updates for Microsoft Exchange Server to address multiple, newly discovered, remote code execution vulnerabilities. Microsoft recommends updating all affected Exchange Servers immediately.

Description

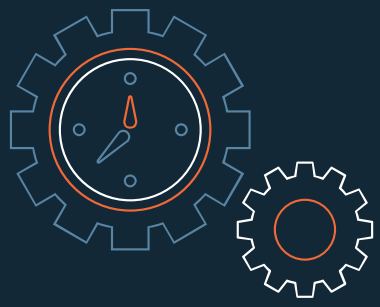
Microsoft released updates for the following vulnerabilities as part of its April 2021 Patch Tuesday: CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, and CVE-2021-28483. The vulnerabilities were first uncovered by the U.S. National Security Agency. Of the vulnerabilities, three are rated as critical and one is rated as high severity. All vulnerabilities can be exploited to perform remote code execution on a server. The most severe vulnerability has the potential to be exploited before authentication. As of today, there have been no known exploitation attempts.

Affected Products

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Safeguards/Recommendations

Affected customers are strongly advised to apply the available patches from Microsoft immediately. Microsoft also recommends that organizations use the Exchange Server Health Checker script to detect common configuration issues and identify servers with missing cumulative or security updates.



Vendor: Microsoft

CVE-ID: Multiple
CVE-2021-28480,
CVE-2021-28481,
CVE-2021-28482,
CVE-2021-28483

Published: April 13, 2021

CVSS V3 Overall score: 9.8, 9.8, 8.8, 9.0

Criticality: Critical, Critical, High, Critical

Patch Availability: Yes

Vulnerability Type: Remote Code Execution

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None, Low

User Interaction: None

Impact Metrics

Scope: Unchanged, Changed

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Unproven

Remediation Level: Official Fix

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io