



Advisory Alert

Alert Number: AAA20210303

Date: March 3, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft Exchange Server	Critical (Important)	Multiple Vulnerabilities

Description

Affected Product	Microsoft Exchange Server
Severity	Critical
Affected Vulnerabilities	Multiple Vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078, CVE-2021-26412, CVE-2021-26854)
Description	<p>Microsoft has released out of band security updates to address multiple vulnerabilities affecting Microsoft Exchange Server.</p> <p>CVE-2021-26855 – A server-side request forgery (SSRF) vulnerability that could allow an attacker to use specially crafted web requests and authenticate as the Exchange Server.</p> <p>CVE-2021-26857 – An insecure deserialization vulnerability in the unified messaging service that could allow an attacker to run code with escalated privileges on the Exchange Server.</p> <p>CVE-2021-26858 and CVE-2021-27065 – Post authentication arbitrary file write vulnerabilities that could allow an authenticated attacker to upload files onto the server.</p> <p>Microsoft highly recommends to apply relevant patches at earliest to avoid issues.</p>
Affected Products	<ul style="list-style-type: none"> • Microsoft Exchange Server 2010 (Service Pack 3) • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2019
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26412</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26854</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27078</p> <p>https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/</p>

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka

Hotline: + 94 112039777

Public Circulation Permitted | Public

Report incident to incident@fincsirt.lk

TLP: WHITE