Advisory Alert

Alert Number: AAA20210414 **Date:** April 14, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft Exchange Server	**Critical**	Remote Code Execution
Microsoft	**High**	Multiple vulnerability

Description

Affected Product	Microsoft Exchange Server
Severity	**Critical -** Initial advisory alert AAA20210303 release date was in 3rd of March 2021, it is again added as a reminder and the update is sent as there are exploitation attempts of this vulnerability in the world.
Affected Vulnerability	Remote Code Execution (CVE-2021-28480 ,CVE-2021-28481)
Description	Microsoft has released security updates addressing remote code execution vulnerabilities that exists in their products. Attackers are using these flaws to compromise Microsoft exchange servers that are exposed to internet allowing access to user accounts and associated networks. According to Microsoft, the patches previously released by them in March 2021 do not remediate these new vulnerabilities and organisations must apply Microsoft's 13 April 2021 updates to prevent potential compromise.
Affected Products	Microsoft Exchange Server 2013 Microsoft Exchange Server 2016 Microsoft Exchange Server 2019
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28480 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28481

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple vulnerability
Description	Microsoft has released its April 2021 Security Updates addressing multiple vulnerabilities that exists across windows operating systems and other softwares. A remote attacker can exploit some of these vulnerabilities to take control of an affected system..
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Apr

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.