# Advisory Alert

**Alert Number:** AAA20210325 **Date:** March 25, 2021

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| Microsoft | **Critical** | Multiple Vulnerabilities |
| Cisco | **Critical** | Arbitrary program execution |
| Cisco | **High** | Multiple Vulnerabilities |
| Redhat | **Medium** | Denial of service |

## Description

| | |
|---|---|
| Affected Product | Microsoft |
| 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 | Multiple Vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065,CVE-2021-27078, CVE-2021-26412, CVE-2021-26854) |
| Description | Microsoft has released out of band security updates to address multiple vulnerabilities affecting Microsoft Exchange Server.<br>**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.<br>**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.<br>**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.<br><br>Microsoft highly recommends to apply relevant patches at earliest to avoid issues. |
| Affected Products | Microsoft Exchange Server 2010 (Service Pack 3)<br>Microsoft Exchange Server 2013<br>Microsoft Exchange Server 2016<br>Microsoft Exchange Server 2019 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26412<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26854<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27078<br>https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchangeserver/ |

| | |
|---|---|
| Affected Product | Cisco |
| Severity | **Critical** |
| Affected Vulnerability | Arbitrary program execution (CVE-2021-1411,CVE-2021-1417,CVE-2021-1418,CVE-2021-1469,CVE-2021-1471) |
| Description | Cisco has released security patch updates addressing vulnerabilities that exists in their products. This vulnerability could allow an attacker to execute arbitrary programs on the under laying OS with elevated privileges and access sensitive information, intercept protected network traffic or cause denial of service. |
| Affected Products | Cisco Jabber for Windows<br>Cisco Jabber for MacOS<br>Cisco Jabber for mobile platforms |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-jabber-PWrTATTC |

| | |
|---|---|
| Affected Product | Cisco |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Cisco has released security patch updates addressing vulnerabilities that exists in their products such as arbitrary code execution, privilege escalation, denial of service etc. Cisco recommends installing necessary patch updates at earliest to avoid issues. |
| Affected Products | Multiple Cisco products |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&impact=critical,high,medium&last_published=2021%20Mar&sort=-last_published#~Vulnerabilities |

| | |
|---|---|
| Affected Product | Redhat |
| Severity | **Medium** |
| Affected Vulnerability | Denial of service (CVE-2020-27827) |
| Description | Redhat has released security updates addressing vulnerability that exists in their products. Specially crafted LLDP packets by an attacker could cause memory to be lost when allocating data to handle specific optional TLVs and affect the system availability. |
| Affected Products | Red Hat Virtualization 4 for RHEL 8 x86_64<br>Red Hat Virtualization Host 4 for RHEL 8 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2021:0976<br>https://access.redhat.com/security/cve/CVE-2020-27827 |

**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.**