TLP: WHITE

Advisory Alert

Alert Number : AAA20201111 **Date :** November 11, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Intel	**High**	Multiple Vulnerabilities
Cisco	**High**	Denial of service

Description

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft released November 2020 security patch updates for multiple vulnerabilities that has been discovered in their products, the most severe flaw of which could allow for remote code execution. Successful exploitations of the most severe of these vulnerabilities could lead an attacker for denial of service, elevation of privilege, security restriction bypass, information disclosure, spoofing and data manipulation. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Microsoft Windows Microsoft Office and Microsoft Office Services and Web Apps Internet Explorer Microsoft Edge (EdgeHTML-based) Microsoft Edge (Chromium-based) ChakraCore Microsoft Exchange Server Microsoft Dynamics Microsoft Windows Codecs Library Azure Sphere Windows Defender Microsoft Teams Azure SDK Azure DevOps Visual Studio
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2020-Nov

Affected Product	Intel
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has released security patch updates addressing multiple vulnerabilities which belongs to firmware, hardware and software advisory categories. Successful exploitation of these vulnerabilities could cause Escalation of Privilege, Denial of Service, Information Disclosure effects on the systems. It is highly recommended to apply necessary security patches to your intel products at earliest to avoid issues.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/default.html

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Denial of service (CVE-2020-26070)
Description	Cisco has released security updates addressing denial of service vulnerability in ingress packet processing function of Cisco XR software for Cisco ASR9000 series aggregation service routers. This is caused due to improper resource allocation when an affected device process network traffic in software switching mode. The attacker could use this flaw and exploit by sending specific streams of L2 or L3 protocol data units that particular device and cause run out of buffer resources. It is highly recommended to apply necessary fixes at earliest.
Affected Products	Cisco ASR 9000 Series Aggregation Services Routers with Cisco IOS XR Software earlier than 6.7.2 or 7.1.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cp-dos-ej8VB9QY

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
Report incident to incident@fincsirt.lk