Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 18 October 2022

Microsoft Releases Patch for Windows TLS Handshake Failures

Severity Level: High

Affected Systems: Microsoft Windows

- Client: Windows 11, version 22H2; Windows 11, version 21H2; Windows 10, version 21H2; Windows 10, version 21H1; Windows 10, version 20H2; Windows 10 Enterprise LTSC 2019; Windows 10 Enterprise LTSC 2016; Windows 10 Enterprise 2015 LTSB; Windows 8.1; Windows 7 SP1

- Server: Windows Server 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 SP1

Description:

A vulnerability has been identified in Microsoft Windows client and server platforms and this can affect some types of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections. These connections might have handshake failures. For developers, the affected connections are likely to receive one or more records followed by a partial record with a size of less than 5 bytes within a single input buffer. If the connection fails, the app will receive the error, "SEC_E_ILLEGAL_MESSAGE".

Microsoft has issued an out-of-band (OOB) non-security update to address an issue triggering SSL/TLS handshake failures on client and server platforms.

Workarounds

Microsoft has released updates (standalone and cumulative) to address the vulnerability. They are as follows:

- *Cumulative updates:*
    - Windows 11, version 21H2: KB5020387
    - Windows Server 2022: KB5020436
    - Windows 10, version 20H2; Windows 10, version 21H1; Windows 10, version 22H1; Windows 10 Enterprise LTSC 2021: KB5020435
    - Windows 10 Enterprise LTSC 2019; Windows Server 2019: KB5020438

- *Standalone Updates:*
    - Windows 8.1; Windows Server 2012 R2: KB5020447
    - Windows Server 2012: KB5020449
    - Windows 7 SP1; Windows Server 2008 R2 SP1: KB5020448

Microsoft is still working on a fix for Windows 10 2016 LTSB, Windows Server 2016, and Windows 10 2015 LTSB.

More information about the updates is available on:
https://support.microsoft.com/en-gb/topic/october-17-2022-kb5020387-os-build-22000-1100-out-of-band-5e723873-2769-4e3d-8882-5cb044455a92

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org