مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Microsoft July 2026 Patch Tuesday

Tracking #:432319296

Date:15-07-2026



**TLP: WHITE**

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft has released its July 2026 Patch Tuesday security updates, addressing a record-breaking 570 security vulnerabilities across Windows, Microsoft Office, SharePoint, Active Directory, SQL Server, Hyper-V, Exchange Server, Visual Studio, Dynamics, Azure components, and numerous Windows services.

## TECHNICAL DETAILS:

Microsoft has released its July 2026 Patch Tuesday security updates, addressing a record-breaking 570 security vulnerabilities across Windows, Microsoft Office, SharePoint, Active Directory, SQL Server, Hyper-V, Exchange Server, Visual Studio, Dynamics, Azure components, and numerous Windows services.
Among these vulnerabilities are three zero-day vulnerabilities, including two actively exploited in-the-wild and one publicly disclosed vulnerability affecting Windows BitLocker.
The update includes 59 Critical vulnerabilities, with the majority enabling Remote Code Execution (RCE) and Elevation of Privilege (EoP). Microsoft noted that this unusually large release is partly due to its AI-powered vulnerability discovery platform (MDASH), which is identifying security flaws earlier within the Windows ecosystem.
Organizations should prioritize deployment of these updates, particularly for Active Directory Federation Services (AD FS) and Microsoft SharePoint Server, as both have already been exploited by threat actors.

**Zero-Day Vulnerabilities**
**1. CVE-2026-56155 – Active Directory Federation Services Elevation of Privilege**
**Severity:** Important
**CVSS:** 7.8
**Exploitation Status: Actively Exploited**

- Impact:
  - Allows an authenticated attacker to obtain administrative privileges.
  - Successful exploitation enables privilege escalation within AD FS environments.

**2. CVE-2026-56164 – Microsoft SharePoint Server Elevation of Privilege**
**Severity:** Moderate
**CVSS:** 5.3
**Exploitation Status: Actively Exploited**
**Vulnerability Details**

- Impact:
  - Enables an unauthenticated remote attacker to gain elevated privileges.
  - Exploitation occurs over the network without valid credentials.
  - SharePoint Server 2019
  - SharePoint Server Subscription Edition
- Microsoft recommends enabling **Antimalware Scan Interface (AMSI)** with **Request Body Scan Mode set to Full** to help mitigate exploitation until updates are applied.

**3. CVE-2026-50661 – Windows BitLocker Security Feature Bypass**
**Severity:** Important
**CVSS:** 6.1
**Exploitation Status:** Publicly Disclosed

- Impact:
  - Allows attackers to bypass BitLocker Device Encryption.
  - Enables unauthorized access to encrypted data stored on affected systems.

**Critical RCEs:**

- **CVE-2026-56159** – DHCP Server Service Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-48561** – Microsoft Copilot Remote Code Execution Vulnerability (**CVSS: 9.6 – Critical**)
- **CVE-2026-55944** – Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central (On-Premises) Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-55008** – Microsoft Exchange Server Spoofing Vulnerability (**CVSS: 9.6 – Critical**)
- **CVE-2026-50522** – Microsoft SharePoint Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-58644** – Microsoft SharePoint Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-55040** – Microsoft SharePoint Server Security Feature Bypass Vulnerability (**CVSS: 9.1 – Critical**)
- **CVE-2026-57092** – Microsoft Windows VMSwitch Elevation of Privilege Vulnerability (**CVSS: 9.9 – Critical**)
- **CVE-2026-55010** – Minecraft Bedrock Dedicated Server Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-54990** – Remote Desktop Client Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-56190** – Remote Desktop Protocol Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-42990** – SQL Server ODBC Driver Elevation of Privilege Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-50518** – Windows DHCP Server Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-49172** – Windows FTP Service Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-50380** – Windows GDI+ Remote Code Execution Vulnerability (**CVSS: 9.6 – Critical**)
- **CVE-2026-49798** – Windows Kernel Elevation of Privilege Vulnerability (**CVSS: 9.3 – Critical**)
- **CVE-2026-50447** – Windows Message Queuing Service (MSMQ) Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)
- **CVE-2026-56188** – Windows Server Network Driver Remote Code Execution Vulnerability (**CVSS: 9.8 – Critical**)

## RECOMMENDATIONS:

**Immediate Actions:**

- Immediately deploy the July 2026 Microsoft security updates across all supported Windows systems and Microsoft products.
- Prioritize patching systems running Active Directory Federation Services (AD FS) and Microsoft SharePoint Server due to active exploitation.

- Enable AMSI on SharePoint servers and configure Request Body Scan Mode to Full as an additional mitigation.
- Verify that all Windows endpoints, servers, and virtual machines have successfully installed the latest cumulative security updates.
- Prioritize remediation of internet-facing and business-critical servers before internal assets

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://msrc.microsoft.com/update-guide/releaseNote/2026-jul