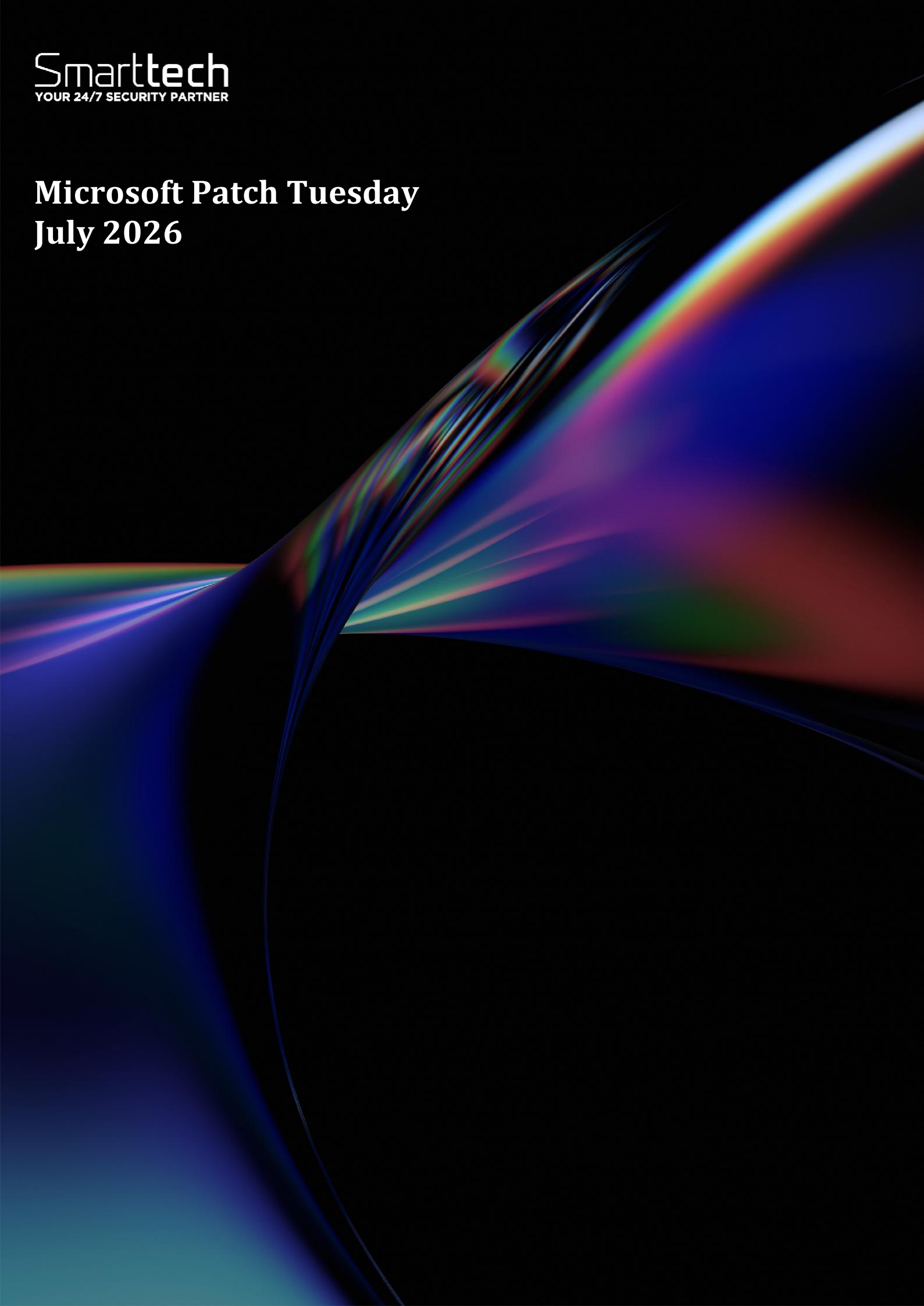
Smarttech
YOUR 24/7 SECURITY PARTNER

Microsoft Patch Tuesday
July 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	114
Authors	Maria-Iasmina Macovei < maria.macovei@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-15
Issue Date	2026-07-14

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Microsoft patched 569 CVEs in its July 2026 Patch Tuesday release, with 56 rated Critical, 510 rated Important, and 3 rated Moderate. This marks the largest Patch Tuesday release in Microsoft's history, surpassing the previous record of 198 CVEs set in June 2026. The release includes three zero-day vulnerabilities, two of which were actively exploited in the wild prior to patch availability, while the third had been publicly disclosed. Elevation of Privilege vulnerabilities accounted for the largest share of this month's updates at 43.8%, followed by Remote Code Execution vulnerabilities at 25.1%, highlighting the continued focus on mitigating high-impact attack vectors across the Microsoft ecosystem.

Risk

Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Medium

Systems Affected:

- .NET
- .NET Core
- .NET Framework
- ASP.NET Core
- Active Directory Certificate Services (AD CS)
- Active Directory Domain Services
- Active Directory Federation Services (AD FS)
- Azure Active Directory
- Azure CycleCloud
- Azure Monitor Agent
- Azure Spring Apps
- Code Integrity DLL (ci.dll)
- Composite Image File System Driver

- Content Delivery Manager
- Desktop Window Manager
- Extensible Storage Engine (ESENT)
- GitHub Copilot and Visual Studio
- GitHub Copilot and Visual Studio Code
- Github Copilot
- HTTP/2
- Microsoft 365 Copilot for iOS
- Microsoft Bing App for IOS
- Microsoft Copilot
- Microsoft Defender
- Microsoft Defender for Endpoint
- Microsoft Dynamics NAV
- Microsoft Edge for Android
- Microsoft Exchange Server
- Microsoft Fabric Data Warehouse
- Microsoft Graphics Component
- Microsoft Input Method Editor (IME)
- Microsoft Install Service
- Microsoft NAT Helper Components (ipnathlp.dll)
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office OneNote
- Microsoft Office PowerPoint
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Printer Drivers
- Microsoft Surface
- Microsoft Windows
- Microsoft Windows App Store
- Microsoft Windows Codecs Library
- Microsoft Windows Media Foundation
- Microsoft Windows Search Component
- Microsoft Windows Speech
- Microsoft XML
- Microsoft XML Core Services
- Minecraft Bedrock Dedicated Server
- Outlook Copilot
- Power BI
- Quality Windows Audio/Video Experience (QWAVE) service
- RPC Runtime
- Reliable Multicast Transport Driver (RMCAST)
- Remote Desktop Client
- Role: DNS Server
- SQL Server

- SQL Server ODBC driver
- Universal Plug and Play (upnp.dll)
- Virtual Hard Disk (VHD) Miniport Driver
- Visual Studio
- Visual Studio Code
- Window PC Manager
- Windows Active Directory
- Windows Admin Center
- Windows Ancillary Function Driver for WinSock
- Windows App Installer
- Windows AppX Deployment Service
- Windows Application Model
- Windows Audio Compression Manager (ACM)
- Windows Audio Service
- Windows Backup Engine
- Windows BitLocker
- Windows Bluetooth Port Driver
- Windows Bluetooth Service
- Windows Boot Loader
- Windows Brokering File System
- Windows Client-Side Caching (CSC) Service
- Windows Clip Service
- Windows Clipboard Server
- Windows Clipboard User Service
- Windows Cloud Files Mini Filter Driver
- Windows Common Log File System Driver
- Windows Connected User Experiences and Telemetry
- Windows Container Isolation FS Filter Driver (unionfs.sys)
- Windows CryptoAPI
- Windows Cryptographic Services
- Windows DHCP Client
- Windows DHCP Server
- Windows DNS
- Windows DWM
- Windows DWM Core Library
- Windows Data.dll
- Windows Devices Human Interface
- Windows DirectX
- Windows Domain Controller
- Windows Event Logging Service
- Windows FTP Service
- Windows File Explorer
- Windows File History Service
- Windows Filtering Platform (WFP)
- Windows GDI

- Windows GDI+
- Windows Graphics Kernel
- Windows Group Policy
- Windows HTTP.sys
- Windows Hyper-V
- Windows Image Acquisition
- Windows Installer
- Windows Internal System User Profile
- Windows Internal Task Bar
- Windows Internet Key Exchange (IKE) Protocol
- Windows Kernel
- Windows Kernel Mode Driver
- Windows Kernel-Mode Drivers
- Windows Key Guard
- Windows LUAFV
- Windows Local Security Authority Subsystem Service (LSASS)
- Windows MIDI Service Module
- Windows Management Services
- Windows Media
- Windows Message Queuing
- Windows Message Queuing Queue Manager
- Windows NTFS
- Windows Narrator Braille
- Windows Netlogon
- Windows Network Address Translation (NAT)
- Windows Network File System
- Windows Network Policy Server SNMP
- Windows Notification
- Windows OLE
- Windows Operating Systems
- Windows Overlay Filter
- Windows PowerShell
- Windows Presentation Foundation (WPF)
- Windows Print Spooler Components
- Windows Projected File System
- Windows Push Notifications
- Windows Quality of Service (QoS) Packet Scheduler
- Windows RDP
- Windows RPC API
- Windows Redirected Drive Buffering
- Windows Remote Access Connection Manager
- Windows Remote Access Service Infrastructure
- Windows Remote Desktop Protocol
- Windows Remote Desktop Services
- Windows Remote Help Defense

- Windows Resilient File System (ReFS)
- Windows Routing and Remote Access Service (RRAS)
- Windows Runtime
- Windows SMB
- Windows SMB Server
- Windows SMB Server Network Transport Driver (srvnet.sys)
- Windows Schannel
- Windows Secure Boot
- Windows Secure Kernel Mode
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows Sensor Data Service
- Windows Server
- Windows Server Backup
- Windows Server Network driver
- Windows Server Update Service
- Windows Spaceport.sys
- Windows StateRepository API
- Windows Storage
- Windows Storage Spaces Direct
- Windows Subsystem for Linux
- Windows System
- Windows TCP/IP
- Windows Telephony Service
- Windows Terminal
- Windows Trusted Runtime Interface Driver
- Windows USB Audio Class driver (usbaudio.sys)
- Windows USB Driver
- Windows USB Hub Driver
- Windows USB Print Driver
- Windows USB Video Driver
- Windows Unified Consent System
- Windows Universal Disk Format File System Driver (UDFS)
- Windows User Interface Core
- Windows VMSwitch
- Windows Virtual Filtering Platform (VFP)
- Windows WalletService
- Windows Web Proxy Auto-Discovery Protocol (WPAD)
- Windows WebView
- Windows Win32K
- Windows Win32K - GRFX
- Windows Wireless Networking
- Windows Wireless Wide Area Network Service

Technology	Products Affected	Severity	Reference	Workaround/ Exploited / Publicly Disclosed	Vulnerability Info
Windows	Windows 10 (multiple versions) Windows 11 (multiple versions) Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2025 Windows Server Core installations	Critical	CVE-2026-56189 CVE-2026-57087 CVE-2026-57094 CVE-2026-57090 CVE-2026-54995 CVE-2026-54982 CVE-2026-54128 CVE-2026-50518 CVE-2026-50370 CVE-2026-56159 CVE-2026-48564 CVE-2026-50382 CVE-2026-49796 CVE-2026-50380 CVE-2026-58542 CVE-2026-50327 CVE-2026-50655	Workaround: No Exploited: No Public: No	Remote Code Execution Elevation of Privilege

			CVE-2026-54992 CVE-2026-58608 CVE-2026-50392 CVE-2026-42982 CVE-2026-50694 CVE-2026-56188 CVE-2026-50444 CVE-2026-54999 CVE-2026-57092		
Microsoft Office	Microsoft 365 Apps for Enterprise Office LTSC 2021 Office LTSC 2024 Office Online Server Microsoft Office Click-To-Run Microsoft Word for Android Microsoft Excel for Android Microsoft PowerPoint for Android Microsoft Outlook for iOS	Critical	CVE-2026-55129 CVE-2026-55049 CVE-2026-55045 CVE-2026-50314 CVE-2026-50467 CVE-2026-55022 CVE-2026-55018 CVE-2026-55140 CVE-2026-55056 CVE-2026-55120	Workaround: No Exploited: No Public: No	Remote Code Execution

			CVE-2026-55043 CVE-2026-55123 CVE-2026-55127 CVE-2026-55033 CVE-2026-55132		
SharePoint	Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016	Critical	CVE-2026-55040 CVE-2026-58644 CVE-2026-50522	Workaround: No Exploited: No Public: No	Remote Code Execution Security Feature Bypass
SQL Server	Microsoft SQL Server 2019 Microsoft SQL Server 2022 SQL Server Analysis Services (SSAS)	Critical	CVE-2026-54118 CVE-2026-54117	Workaround: No Exploited: No Public: No	Remote Code Execution
Exchange	Microsoft Exchange Server 2016 Cumulative Update 23 Microsoft Exchange Server 2019 Cumulative Update 14 and 15 Microsoft Exchange Server Subscription Edition	Critical	CVE-2026-55008	Workaround: No Exploited: No Public: No	Spoofing
Hyper-V	Windows 11 Windows Server 2016 Windows Server 2019	Critical	CVE-2026-50680 CVE-2026-54127	Workaround: No Exploited: No Public: No	Elevation of Privilege

	Windows Server 2022 Windows Server 2025 Server Core installations				
Remote Desktop	Windows 10 Windows 11 Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2025 Server Core installations	Critical	CVE-2026-50474	Workaround: No Exploited: No Public: No	Remote Code Execution
Microsoft Defender / Other Products	Microsoft Defender Microsoft Copilot Microsoft Dynamics NAV Microsoft Dynamics 365 Business Central (On-Premises) Active Directory Certificate Services Active Directory Domain Services Minecraft Bedrock Dedicated Server	Critical	CVE-2026-55012 CVE-2026-55011 CVE-2026-48561 CVE-2026-55944 CVE-2026-54121 CVE-2026-49164 CVE-2026-55010	Workaround: No Exploited: No Public: No	Remote Code Execution Elevation of Privilege

CISA has issued a warning regarding active, in-the-wild exploitation of three vulnerabilities affecting all supported on-premises versions of Microsoft SharePoint Server (Subscription Edition, 2019, and 2016)

CVE	Type	CISA KEV Added Date	Severity / CVSS	Status
CVE-2026-32201	Authentication Bypass / Spoofing	April 14, 2026	Medium (6.5)	Actively Exploited
CVE-2026-45659	Deserialization of Untrusted Data	July 1, 2026	High (8.8)	Actively Exploited
CVE-2026-56164	Missing Authentication / Spoofing	July 14, 2026	Moderate	Actively Exploited
CVE-2026-55040	Security Feature Bypass (Weak Auth)	N/A	Critical	High Risk (Unpatched potential)
CVE-2026-58644	Deserialization Remote Code Execution	N/A	Critical	High Risk (Unpatched potential)

CISA urges organizations to detect and remediate a potential compromise by implementing the following recommendations:

- Apply the latest patches and security updates from Microsoft, verify that installation completes successfully, and shorten patching cycles when possible.
- Verify that Antimalware Scan Interface (AMSI) integration is enabled for each SharePoint web application. Follow Microsoft's Configure AMSI integration with SharePoint Server guidance to ensure proper configuration and select the "Full Mode" option for the Request Body Scan Mode, where feasible. When compromise is expected, use the following AMSI and Microsoft Defender Antivirus (MDAV) detections, and implement your organization's incident response plan for any

positive detections:

- AMSI: Exploit:Script/SuspSignoutReqBody.A – request body scanning; SharePoint Server Subscription only; Microsoft has blocked observed attempts.
- AMSI: Exploit:Script/ToolPaneAuthBypass.A – request header scanning; SharePoint Server 2016, 2019, and Subscription Edition.
- AMSI: Exploit:Script/ToolPaneAuthBypass.C – RCE coverage; SharePoint Server 2016, 2019, and Subscription Edition.
- MDAV: Backdoor:MSIL/LeakFang.A!dha – post-exploitation activity alert involving IIS-protected secrets.

In addition, CISA recommends that organizations implement the following SharePoint Server hardening measures:

- Before rotating IIS machine keys, hunt for and remediate any intrusion artifacts, including machine-key harvesters, that could allow for the keys to be stolen again. Review Microsoft's Improved ASP.NET view state security and key management for best practices.
- Establish tailored logging mechanisms to detect and monitor exploitation activities. Review telemetry for anomalous requests, suspicious SharePoint worker-process activity, webshells, and machine-key access. For more information, see CISA's Best Practices for Event Logging and Threat Detection.
- Avoid exposing SharePoint Servers directly to the internet unless necessary; and if necessary, only configure a SharePoint Server behind a Layer 7 reverse proxy or equivalent application-layer security control that requires authentication and can inspect and filter requests.
- Block external access to SharePoint Central Administration, restrict farm and database communications to required systems, and review Microsoft's SharePoint Server security-hardening guidance for role-specific ports, services, and Web.config settings.

Recommendations

Smarttech247 team recommend the following actions to be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
  - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such

as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response client or host-based IPS agent.

References

Microsoft July 2026 Patch Tuesday fixes massive 570 flaws, 3 zero-days
July 2026 Patch Tuesday: Largest Patch Tuesday 569 CVEs
https://msrc.microsoft.com/update-guide/releaseNote/2026-Jul
CISA Urges SharePoint Hardening After New Exploitations | CISA

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com