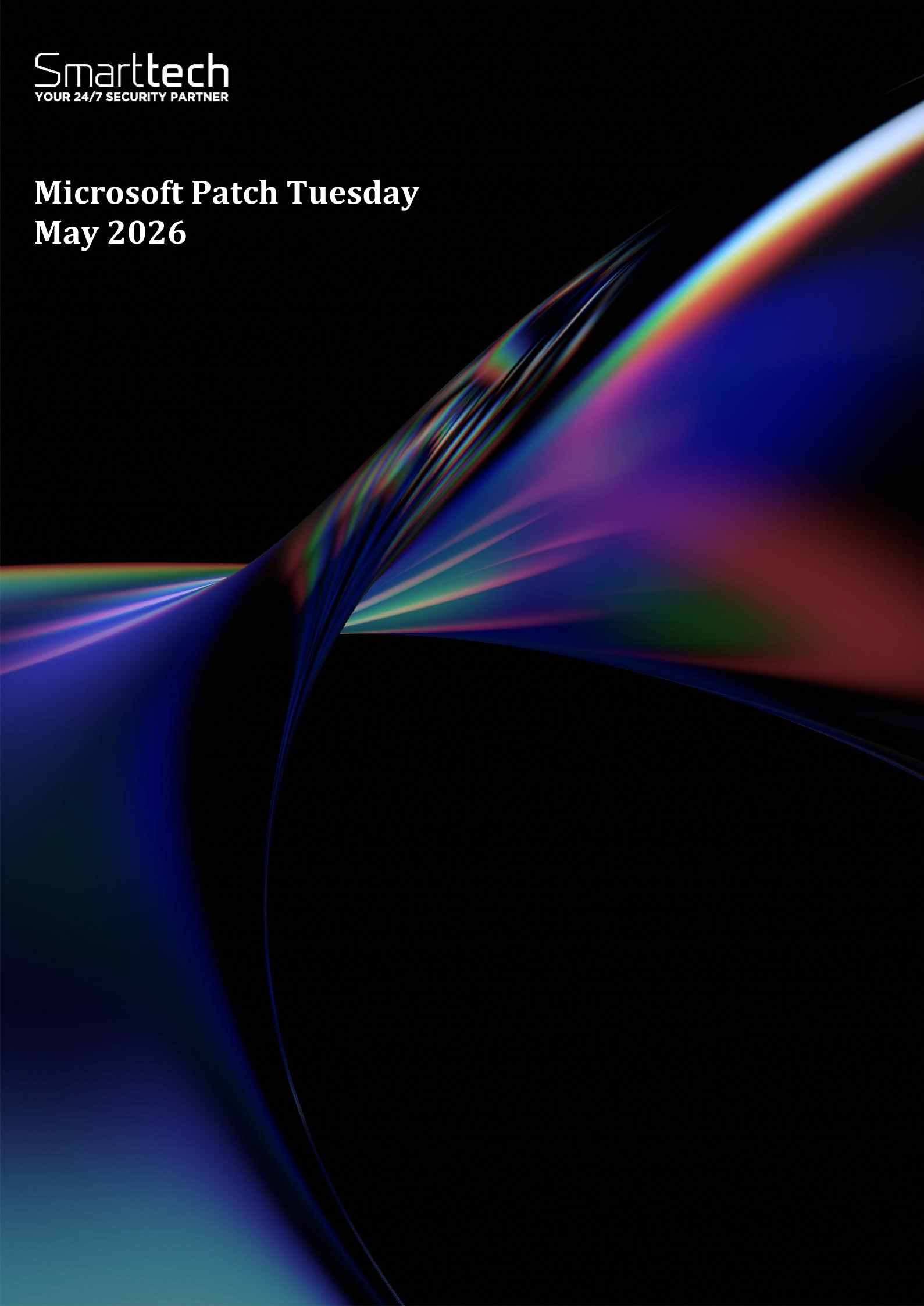
Smarttech
YOUR 24/7 SECURITY PARTNER

Microsoft Patch Tuesday
May 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	71
Authors	Daniel-Cristian Carp < daniel.carp@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-05-13
Issue Date	2026-05-12

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 120 CVEs in its May 2026 Patch Tuesday release. This Patch Tuesday addresses 17 "Critical" vulnerabilities, 14 of which are remote code execution, 2 are elevation of privilege, and 1 is an information disclosure flaw. This release does not include any publicly disclosed zero-day vulnerabilities.

CVE-2026-41103 is an elevation of privilege vulnerability affecting Microsoft Single-Sign-On (SSO) Plugin for Jira & Confluence. It was assigned a CVSSv3 score of 9.1 and is rated as critical. It was assessed as "Exploitation More Likely" according to Microsoft's Exploitability Index. An unauthorized attacker could exploit this vulnerability during the process of logging in by sending a specially crafted response message. Successful exploitation would allow the attacker to sign-in using a forged identity without Microsoft Entra ID authentication, enabling access to or allowing an attacker to modify data in Jira and Confluence. However, the accessible information is not unfettered, as it is limited by the access defined by the targeted servers for the authorized user.

CVE-2026-33841, CVE-2026-35420 and **CVE-2026-40369** are EoP vulnerabilities affecting the Windows Kernel. Each of the flaws have been assigned CVSSv3 scores of 7.8 and rated as important. Both CVE-2026-33841 and CVE-2026-40369 were assessed as "Exploitation More Likely," which could be abused by a local attacker to elevate to SYSTEM or Medium/High integrity level in the case of CVE-2026-33841. Including these three EoPs, there have been 13 disclosed Windows Kernel EoP vulnerabilities addressed so far in 2026.

CVE-2026-40361, CVE-2026-40364, CVE-2026-40366 and **CVE-2026-40367** RCE vulnerabilities affecting Microsoft Word. Each of these RCEs were assigned CVSSv3 scores of 8.4 and rated as critical, though CVE-2026-40361 and CVE-2026-40364 were the only ones assessed to be “Exploitation More Likely.” An attacker could exploit these flaws through social engineering by sending the malicious file to an intended target. Successful exploitation would grant code execution privileges to the attacker. Additionally, Microsoft notes that the Preview Pane is an attack vector for each of these vulnerabilities.

CVE-2026-41089 is a RCE vulnerability affecting Windows Netlogon, a Windows Server process used for authentication within a domain. It was assigned a CVSSv3 score of 9.8 and rated as critical. A remote, unauthenticated attacker could exploit this flaw by sending a crafted network request to a Windows server running as a domain controller. This packet could exploit a stack-based buffer overflow flaw, allowing the attacker to execute code on an affected system. Despite the critical severity and near perfect CVSSv3 score, this flaw was

assessed by Microsoft as “Exploitation Less Likely.”

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
- ASP.NET Core
- Azure AI Foundry M365 published agents
- Azure Cloud Shell
- Azure Connected Machine Agent
- Azure DevOps
- Azure Entra ID
- Azure Logic Apps
- Azure Machine Learning
- Azure Managed Instance for Apache Cassandra
- Azure Monitor Agent
- Azure Notification Service
- Azure SDK
- Copilot Chat (Microsoft Edge)
- Data Deduplication
- Dynamics Business Central
- GitHub Copilot and Visual Studio
- M365 Copilot
- M365 Copilot for Desktop
- Microsoft Data Formulator
- Microsoft Dynamics 365 (on-premises)
- Microsoft Dynamics 365 Customer Insights
- Microsoft Edge (Chromium-based)
- Microsoft Edge for Android
- Microsoft Office
- Microsoft Office Click-To-Run
- Microsoft Office Excel
- Microsoft Office PowerPoint
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Partner Center
- Microsoft SSO Plugin for Jira & Confluence
- Microsoft Teams

- Microsoft Windows DNS
- Power Automate
- SQL Server
- Telnet Client
- Visual Studio Code
- Windows Admin Center
- Windows Ancillary Function Driver for WinSock
- Windows Application Identity (AppID) Subsystem
- Windows Cloud Files Mini Filter Driver
- Windows Common Log File System Driver
- Windows Cryptographic Services
- Windows DWM Core Library
- Windows Event Logging Service
- Windows Filtering Platform (WFP)
- Windows GDI
- Windows Hyper-V
- Windows Internet Key Exchange (IKE) Protocol
- Windows Kernel
- Windows Kernel-Mode Drivers
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Link-Layer Discovery Protocol (LLDP)
- Windows Message Queuing
- Windows Native WiFi Miniport Driver
- Windows Netlogon
- Windows Print Spooler Components
- Windows Projected File System
- Windows Remote Desktop
- Windows Rich Text Edit
- Windows Rich Text Edit Control
- Windows SMB Client
- Windows Secure Boot
- Windows Storage Spaces Controller
- Windows Storport Miniport Driver
- Windows TCP/IP
- Windows Telephony Service
- Windows Volume Manager Extension Driver
- Windows Win32K - GRFX
- Windows Win32K - ICOMP

Technology	Products Affected	Severity	Reference	Workaround/ Exploited / Publicly Disclosed	Vulnerability Info
Windows	Windows Server 2012, 2012 R2, 2016, 2019, 2022, 2025 including Server Core Installations Windows 10, 11 Windows Admin Center in Azure Portal Windows Admin Center	Critical	CVE-2026-41095 CVE-2026-35423 CVE-2026-41086 CVE-2026-35438 CVE-2026-35416 CVE-2026-41088 CVE-2026-34345 CVE-2026-34344 CVE-2026-34343 CVE-2026-34337 CVE-2026-35418 CVE-2026-33835 CVE-2026-40397 CVE-2026-40407 CVE-2026-40377 CVE-2026-34336 CVE-2026-42896	Workaround: No Exploited: No Public: No	Elevation of Privilege Information Disclosure Security Feature Bypass Remote Code Execution Denial of Service

			CVE-2026-35419 CVE-2026-33834 CVE-2026-32209 CVE-2026-35421 CVE-2026-40402 CVE-2026-35424 CVE-2026-40369 CVE-2026-33841 CVE-2026-35420 CVE-2026-34332 CVE-2026-40408 CVE-2026-34339 CVE-2026-34341 CVE-2026-34329 CVE-2026-33838 CVE-2026-32161 CVE-2026-41089 CVE-2026-34342 CVE-2026-34340		

			CVE-2026-40398 CVE-2026-21530 CVE-2026-32170 CVE-2026-41097 CVE-2026-40410 CVE-2026-35415 CVE-2026-34350 CVE-2026-34351 CVE-2026-33837 CVE-2026-40406 CVE-2026-40414 CVE-2026-34334 CVE-2026-40399 CVE-2026-35422 CVE-2026-40413 CVE-2026-40415 CVE-2026-40401 CVE-2026-40405 CVE-2026-40382		

			CVE-2026-34338 CVE-2026-42825 CVE-2026-40380 CVE-2026-33839 CVE-2026-40403 CVE-2026-34347 CVE-2026-34333 CVE-2026-34330 CVE-2026-34331 CVE-2026-35417 CVE-2026-33840		
Office	Microsoft Outlook for iOS M365 Copilot for Desktop Microsoft Office LTSC Microsoft Excel for Android Microsoft Word for Android Microsoft 365 Apps for Enterprise Office Online Server Microsoft PowerPoint for Android Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019	Critical	CVE-2026-41100 CVE-2026-42893 CVE-2026-26164 CVE-2026-41614 CVE-2026-42832 CVE-2026-42831 CVE-2026-40363 CVE-2026-40419	Workaround: No Exploited: No Public: No	Spoofing Tampering Information Disclosure Remote Code Execution Elevation of Privilege

	Microsoft SharePoint Server Subscription Edition		CVE-2026-40358 CVE-2026-35436 CVE-2026-40420 CVE-2026-40418 CVE-2026-40360 CVE-2026-40362 CVE-2026-40359 CVE-2026-41102 CVE-2026-40361 CVE-2026-40367 CVE-2026-35440 CVE-2026-40421 CVE-2026-41101 CVE-2026-40366 CVE-2026-40364		
SQL Server	2016 SP3 GDR, Azure Connect Feature Pack 2017 RTM+GDR 2017 CU31+GDR 2019 RTM+GDR 2019 CU32+GDR 2022 RTM+GDR	Important	CVE-2026-40370	Workaround: No Exploited: No Public: No	Remote Code Execution

	2022 CU24+GDR 2025 RTM+GDR 2025 CU4+GDR				
SharePoint	Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016	Critical	CVE-2026-40368 CVE-2026-35439 CVE-2026-33112 CVE-2026-40365 CVE-2026-40357 CVE-2026-33110	Workaround: No Exploited: No Public: No	Remote Code Execution
Azure	Azure Connected Machine Agent Azure Logic Apps Azure Machine Learning Azure Monitor Agent Azure Monitor Agent Metrics Extension Azure SDK for Java	Important	CVE-2026-40381 CVE-2026-42823 CVE-2026-33833 CVE-2026-32204 CVE-2026-42830 CVE-2026-33117	Workaround: No Exploited: No Public: No	Elevation of Privilege Spoofing Security Feature Bypass
.Net	.NET 8.0, 9.0, 10.0 installed on Windows, Mac OS, Linux .NET Framework 3.5, 4.8, 4.8.1, 4.6.2/4.7/4.7.1/4.7.2 Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)	Important	CVE-2026-35433 CVE-2026-32177 CVE-2026-32175 CVE-2026-42899	Workaround: No Exploited: No Public: No	Elevation of Privilege Core Tampering Core Denial of Service

	Microsoft Visual Studio 2022 version 17.12 Microsoft Visual Studio 2022 version 17.14 Microsoft Visual Studio 2026 version 18.5				
Developer Tools	Visual Studio Code Visual Studio Code - Live Preview extension	Important	CVE-2026-41109 CVE-2026-41613 CVE-2026-41612 CVE-2026-41610 CVE-2026-41611	Workaround: No Exploited: No Public: No	Security Feature Bypass Elevation of Privilege Information Disclosure Remote Code Execution
Business Applications	Microsoft Dynamics 365 Business Central 2024 Release Wave 2, 2025 Release Wave 1&2, 2026 Release Wave 1. Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Teams for Android Power Automate for Desktop	Critical	CVE-2026-40417 CVE-2026-42898 CVE-2026-42833 CVE-2026-32185 CVE-2026-40374	Workaround: No Exploited: No Public: No	Elevation of Privilege Remote Code Execution Information Disclosure
Microsoft Windows DNS	Windows 11 Windows Server 2025	Critical	CVE-2026-41096	Workaround: No Exploited: No Public: No	Remote Code Execution
Microsoft SSO Plugin for Jira & Confluence	Microsoft Confluence SAML SSO plugin 7.4.0 Microsoft JIRA SAML SSO plugin 1.3.3	Critical	CVE-2026-41103	Workaround: No Exploited: No Public: No	Elevation of Privilege
Other	Microsoft Data Formulator 0.7	Critical	CVE-2026-41094	Workaround: No Exploited: No Public: No	Remote Code Execution

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 (EDR) client or host-based IPS agent.

References

https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2026-patch-tuesday-fixes-120-flaws-no-zero-days/

https://www.tenable.com/blog/microsofts-may-2026-patch-tuesday-addresses-118-cves-cve-2026-41103

CVE

CVE-2026-41095
CVE-2026-35423
CVE-2026-41086
CVE-2026-35438
CVE-2026-35416
CVE-2026-41088
CVE-2026-34345
CVE-2026-34344
CVE-2026-34343
CVE-2026-34337
CVE-2026-35418
CVE-2026-33835
CVE-2026-40397
CVE-2026-40407
CVE-2026-40377
CVE-2026-34336
CVE-2026-42896
CVE-2026-35419
CVE-2026-33834
CVE-2026-32209
CVE-2026-35421
CVE-2026-40402
CVE-2026-35424
CVE-2026-40369
CVE-2026-33841
CVE-2026-35420
CVE-2026-34332
CVE-2026-40408
CVE-2026-34339
CVE-2026-34341
CVE-2026-34329
CVE-2026-33838
CVE-2026-32161
CVE-2026-41089
CVE-2026-34342
CVE-2026-34340
CVE-2026-40398
CVE-2026-21530
CVE-2026-32170
CVE-2026-41097
CVE-2026-40410
CVE-2026-35415
CVE-2026-34350
CVE-2026-34351
CVE-2026-33837
CVE-2026-40406

CVE-2026-40414
CVE-2026-34334
CVE-2026-40399
CVE-2026-35422
CVE-2026-40413
CVE-2026-40415
CVE-2026-40401
CVE-2026-40405
CVE-2026-40382
CVE-2026-34338
CVE-2026-42825
CVE-2026-40380
CVE-2026-33839
CVE-2026-40403
CVE-2026-34347
CVE-2026-34333
CVE-2026-34330
CVE-2026-34331
CVE-2026-35417
CVE-2026-33840
CVE-2026-41100
CVE-2026-42893
CVE-2026-26164
CVE-2026-41614
CVE-2026-42832
CVE-2026-42831
CVE-2026-40363
CVE-2026-40419
CVE-2026-40358
CVE-2026-35436
CVE-2026-40420
CVE-2026-40418
CVE-2026-40360
CVE-2026-40362
CVE-2026-40359
CVE-2026-41102
CVE-2026-40361
CVE-2026-40367
CVE-2026-35440
CVE-2026-40421
CVE-2026-41101
CVE-2026-40366
CVE-2026-40364
CVE-2026-40370
CVE-2026-40368
CVE-2026-35439
CVE-2026-33112
CVE-2026-40365
CVE-2026-40357
CVE-2026-33110
CVE-2026-40381
CVE-2026-42823
CVE-2026-33833
CVE-2026-32204
CVE-2026-42830
CVE-2026-33117
CVE-2026-35433

CVE-2026-32177
CVE-2026-32175
CVE-2026-42899
CVE-2026-41109
CVE-2026-41613
CVE-2026-41612
CVE-2026-41610
CVE-2026-41611
CVE-2026-40417
CVE-2026-42898
CVE-2026-42833
CVE-2026-32185
CVE-2026-40374
CVE-2026-41096
CVE-2026-41103
CVE-2026-41094

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com