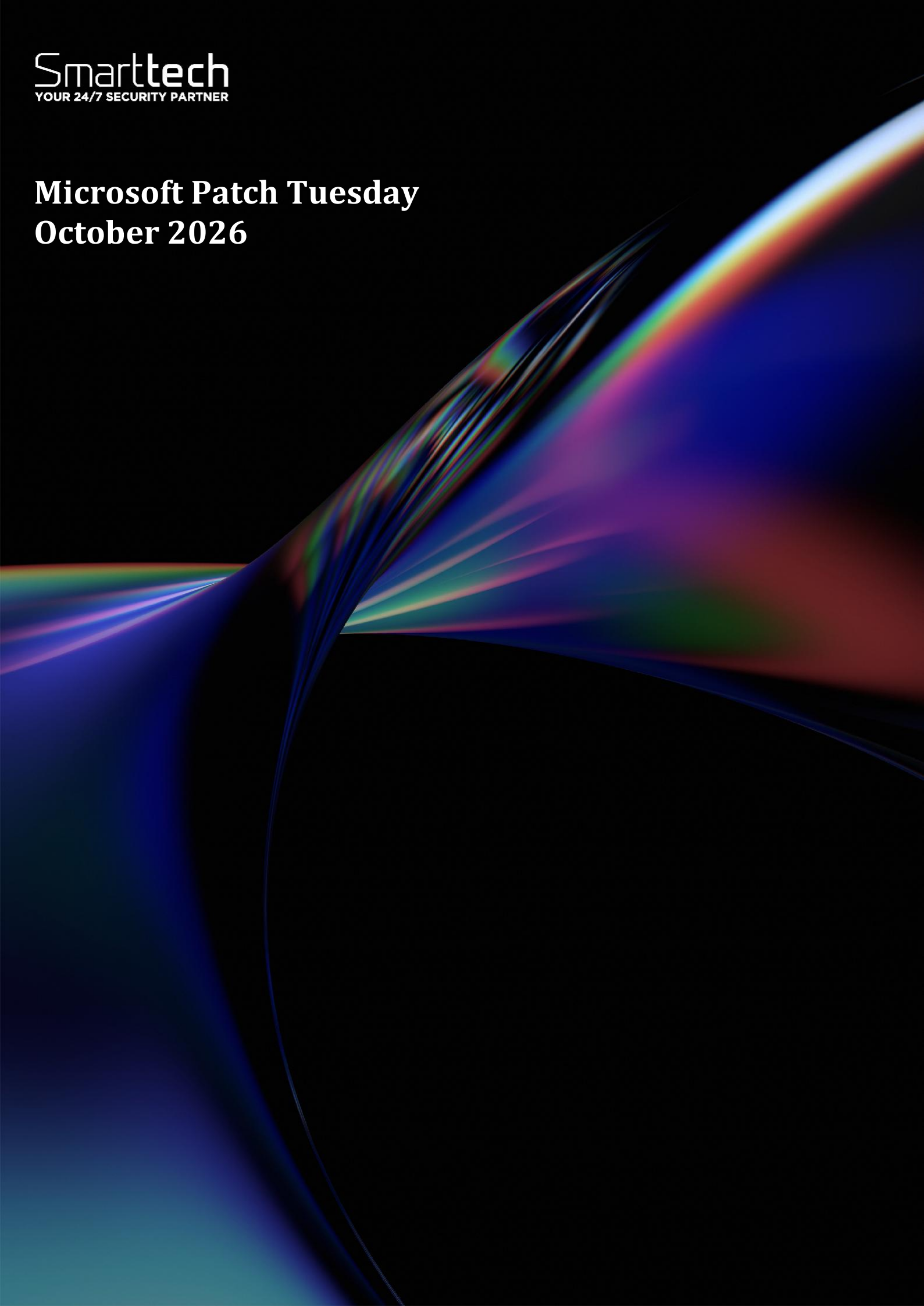


Microsoft Patch Tuesday October 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	174
Authors	Mihai Butoi < mihai.butoi@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-14
Issue Date	2026-10-13

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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's October 2026 Patch Tuesday release addresses a record-breaking number of security vulnerabilities, with reports identifying 1,411 flaws, including 70 rated Critical. Among the Critical vulnerabilities, 57 involve remote code execution (RCE), 11 involve elevation of privilege (EoP), and two involve spoofing. The release also addresses one actively exploited zero-day vulnerability and two publicly disclosed zero-day vulnerabilities. By vulnerability category, elevation of privilege accounts for the largest share, with approximately 677 flaws, followed by remote code execution (317), information disclosure (254), denial of service (73), security feature bypass (40), and spoofing (28). These figures reflect the reported Patch Tuesday count; broader October totals may differ depending on whether vulnerabilities fixed in earlier releases during the month are included.

Key security developments:

- **Active exploitation:** CVE-2026-96951, a Windows Shell security feature bypass, was exploited in the wild. It allows attackers to bypass Mark of the Web protections.
- **Public disclosure:** CVE-2026-108398 affects .NET Framework and could allow unauthorized applications to run by bypassing Windows Defender Application Control (WDAC) restrictions.
- **Public disclosure:** CVE-2026-92707 affects MessagePack-CSharp and is a denial-of-service vulnerability.
- **End of support:** Windows 11 version 24H2 Home and Pro, and Windows 10 Enterprise LTSB 2016, reached the end of updates on 13 October 2026. Microsoft identifies the October security update as the final update for these editions.

Risk

Government:

- Large and medium-sized government entities: **High**
- Small government entities: **High**

Businesses:

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

Home users: High

Systems Affected:

- *Windows 10 and Windows 11
- *Windows Server
- *Windows Shell
- *Windows Kernel and core system components
- *Desktop Window Manager
- *Windows Search Component and Windows Search Service
- *Windows Media Foundation
- *Windows Codecs Library and HEVC Video Extensions
- *Windows PDF
- *Windows Scripting Engine
- *Windows installation, deployment, and update services
- *Windows filesystems, storage, and backup components
- *Windows graphics, media, and content-processing components
- *Connected Devices Platform Service
- *Microsoft Streaming Service
- *Microsoft QUIC
- *.NET
- *.NET Framework
- *ASP.NET Core
- *Visual Studio
- *MessagePack-CSharp
- *Microsoft PowerToys
- *Azure Active Directory
- *Azure API Center
- *Azure App Service
- *Azure Arc
- *Azure CycleCloud
- *Azure DevOps
- *Azure Event Grid
- *Azure HDInsight
- *Azure Key Vault
- *Azure SRE Agent
- *Azure Storage Library
- *Microsoft Azure Attestation Service
- *Device Health Attestation Service
- *Microsoft Office and related document and mail-client components
- *Microsoft Dynamics 365 Business Central
- *Microsoft Exchange Server
- *Microsoft Bookings
- *Microsoft Dataverse

*Microsoft Partner Center

*Microsoft Mariner (Linux-based platform)

*Active Directory and other Windows identity and authentication components

Technology	Products Affected	Severity	Reference	Workaround/ Exploited / Publicly Disclosed	Vulnerability Info
Active Directory Domain Services	Active Directory Domain Services	Critical	CVE-2026-70229	No exploitation	Remote code execution
Active Directory Federation Services	Active Directory Federation Services	Critical	CVE-2026-96222, CVE-2026-108131	No exploitation	Spoofing
Azure API Center	Azure API Center	Critical	CVE-2026-83943	Earlier-month fix; no exploitation	Information disclosure
Azure App Service	Azure App Service	Critical	CVE-2026-77900	Earlier-month fix; no exploitation	Remote code execution
Azure Event Grid	Azure Event Grid	Critical	CVE-2026-83947	Earlier-month fix; no exploitation	Spoofing
Azure SRE Agent	Azure SRE Agent	Critical	CVE-2026-69435	Earlier-month fix; no exploitation	Elevation of privilege
Linux Kernel	Linux Kernel	Critical	CVE-2026-62840	No exploitation	Elevation of privilege
Microsoft Bookings	Microsoft Bookings	Critical	CVE-2026-94510	Earlier-month fix; no exploitation	Elevation of privilege
Microsoft Dataverse	Microsoft Dataverse	Critical	CVE-2026-88131	Earlier-month fix; no exploitation	Remote code execution
Microsoft Exchange Server	Exchange Server	Critical	CVE-2026-70571	Earlier-month fix; no exploitation	Remote code execution

Microsoft Graphics Component	Microsoft Graphics Component	Critical	CVE-2026-100215	No exploitation	Remote code execution
Microsoft Excel	Microsoft Excel	Critical	CVE-2026-105718, CVE-2026-100209, CVE-2026-100210, CVE-2026-100211, CVE-2026-97739, CVE-2026-97741, CVE-2026-97742, CVE-2026-97745, CVE-2026-97753, CVE-2026-97755, CVE-2026-97756, CVE-2026-97758, CVE-2026-97759, CVE-2026-97761, CVE-2026-97765, CVE-2026-97767, CVE-2026-97776, CVE-2026-97778, CVE-2026-97780	No exploitation	Remote code execution
Microsoft Outlook	Microsoft Outlook	Critical	CVE-2026-70242, CVE-2026-70291, CVE-2026-88156, CVE-2026-97016, CVE-2026-97749	No exploitation	Remote code execution
Microsoft PowerPoint	Microsoft PowerPoint	Critical	CVE-2026-88178, CVE-2026-70215, CVE-2026-	No exploitation	Remote code execution

			88144, CVE-2026- 88207		
Microsoft SharePoint	SharePoint Server	Critical	CVE-2026- 102866	No exploitation	Elevation of privilege
Microsoft Visio	Microsoft Visio	Critical	CVE-2026- 102855, CVE-2026- 102856, CVE-2026- 102857	No exploitation	Remote code execution
Microsoft Word	Microsoft Word	Critical	CVE-2026- 70269, CVE-2026- 88185, CVE-2026- 70300	No exploitation	Remote code execution
Microsoft Mariner	Mariner Linux distribution and affected packages	Critical	CVE-2026- 78663 CVE-2026- 98301 CVE-2026- 98304 CVE-2026- 98303 CVE-2026- 98292 CVE-2026- 98298 CVE-2026- 98295 CVE-2026- 98320 CVE-2026- 98319 CVE-2026- 98317 CVE-2026- 98323 CVE-2026- 98322 CVE-2026- 98321 CVE-2026- 98311 CVE-2026- 98308 CVE-2026- 98316 CVE-2026- 98269 CVE-2026- 98272 CVE-2026- 98270 CVE-2026-	No exploitation	Multiple Critical-rated Linux kernel and package vulnerabilities

			98289 CVE-2026-98288 CVE-2026-98279 CVE-2026-98255 CVE-2026-98179 CVE-2026-98180 CVE-2026-98174 CVE-2026-98176 CVE-2026-98177 CVE-2026-98181 CVE-2026-98187 CVE-2026-98215 CVE-2026-98186 CVE-2026-98203 CVE-2026-98170 CVE-2026-98206 CVE-2026-98168 CVE-2026-98199 CVE-2026-98207 CVE-2026-98167 CVE-2026-98171 CVE-2026-98172 CVE-2026-98209 CVE-2026-98212 CVE-2026-98211 CVE-2026-98217 CVE-2026-98192 CVE-2026-98193		
Microsoft Partner	Partner Center	Critical	CVE-2026-96207	Earlier-month fix; no	Elevation of

Center				exploitation	privilege
Windows GDI+	Windows GDI+	Critical	CVE-2026-83934	No exploitation	Remote code execution
Windows Graphics Kernel	Windows Graphics Kernel	Critical	CVE-2026-88073	No exploitation	Elevation of privilege
Windows Hyper-V	Windows Hyper-V	Critical	CVE-2026-108399, CVE-2026-102214, CVE-2026-105733	No exploitation	Elevation of privilege / remote code execution
Windows Kernel	Windows Kernel	Critical	CVE-2026-96913	No exploitation	Elevation of privilege
Windows Media Foundation	Windows Media Foundation	Critical	CVE-2026-96952	No exploitation	Remote code execution
Windows Media Video Decoder	Windows Media Video Decoder	Critical	CVE-2026-100220	No exploitation	Remote code execution
Windows Message Queuing	Windows Message Queuing	Critical	CVE-2026-108460, CVE-2026-100202	No exploitation	Remote code execution
Windows Raw Image Extension	Windows Raw Image Extension	Critical	CVE-2026-96943, CVE-2026-96202, CVE-2026-21413	No exploitation	Remote code execution
Windows Text Shaping	Windows Text Shaping	Critical	CVE-2026-97814, CVE-2026-102225	No exploitation	Remote code execution
Windows Virtualization-Based Security	Windows VBS Enclave	Critical	CVE-2026-108471, CVE-2026-88074, CVE-2026-96914, CVE-2026-102211, CVE-2026-108130	No exploitation	Elevation of privilege
Windows PostScript Printer Driver	Windows PostScript Printer Driver	Critical	CVE-2026-70147, CVE-2026-70153, CVE-2026-108467	No exploitation	Remote code execution

Microsoft QUIC	Microsoft QUIC	Critical	CVE-2026-100219, CVE-2026-105016	No exploitation	Remote code execution
Windows PDF	Windows PDF	Critical	CVE-2026-108457	No exploitation	Remote code execution
Network Device Enrollment Service	NDES	Critical	CVE-2026-69802	No exploitation	Remote code execution
Windows ALPC	Windows ALPC	Critical	CVE-2026-83917	No exploitation	Elevation of privilege
Windows Deployment Services	Windows Deployment Services	Critical	CVE-2026-88174	No exploitation	Remote code execution
Windows DHCP Client	Windows DHCP Client	Critical	CVE-2026-70250	No exploitation	Remote code execution
Windows DHCP Server	Windows DHCP Server	Critical	CVE-2026-96934, CVE-2026-88117, CVE-2026-88119, CVE-2026-88120, CVE-2026-88171	No exploitation	Remote code execution
Windows Reliable Multicast Transport Driver	RMCAST	Critical	CVE-2026-69789	No exploitation	Remote code execution
Windows Remote Desktop Services	Remote Desktop Services / Gateway	Critical	CVE-2026-70187	No exploitation	Remote code execution
HEVC Video Extensions	HEVC Video Extensions	Critical	CVE-2026-108400	No exploitation	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 client or host-based IPS agent.

References

<https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days/>

<https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-October-2026.html>

<https://support.microsoft.com/en-gb/servicing/os/windows-11/2026/10/kb5127648-windows-11-24h2-25h2-26h2-security-update>

