Smarttech
YOUR 24/7 SECURITY PARTNER

Microsoft Patch Tuesday
February 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	23
Authors	Teodora Diaconescu <teodora.diaconescu@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-11
Issue Date	2026-02-10

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 58 CVEs in its February 2026 Patch Tuesday release, including 6 actively exploited and three publicly disclosed zero-day vulnerabilities. This Patch Tuesday also addresses five Critical vulnerabilities, 3 of which are elevation of privileges flaws and 2 information disclosure flaws.

CVE-2026-21510 is a security feature bypass vulnerability affecting Windows Shell. It was assigned a CVSSv3 score of 8.8 and was rated as important. According to Microsoft, this flaw was publicly disclosed prior to a patch being made available and was also exploited in the wild as a zero-day. Exploitation requires an attacker to convince an unsuspecting user to open a malicious link or shortcut file. This would allow the attacker to bypass Windows SmartScreen and Windows Shell warnings by exploiting a flaw in Windows Shell components.

CVE-2026-21513 is a security feature bypass vulnerability in the MSHTML Framework. It was assigned a CVSSv3 score of 8.8 and rated as important. According to Microsoft, it was both exploited in the wild and publicly disclosed prior to a patch being available. Successful exploitation of this flaw requires an attacker to convince a potential victim into opening either a malicious HTML file or a shortcut (.lnk) file. Like similar security feature bypass flaws, this vulnerability can bypass protection prompts that would caution a user before opening a file.

CVE-2026-21514 is a security feature bypass vulnerability affecting Microsoft Word. It was assigned a CVSSv3 score of 7.8 and rated as important. Successful exploitation requires an attacker to convince a user to open a crafted Office file. According to the Microsoft advisory, the preview pane is not an attack vector. This vulnerability was publicly disclosed prior to a patch being made available and was also exploited in the wild as a zero-day. Microsoft credited the discovery of this vulnerability to an Anonymous researcher, Google Threat Intelligence Group, Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC) and Office Product Group Security Team.

CVE-2026-21519 is an EoP vulnerability affecting Desktop Window Manager, a Windows service used to render the graphical user interface (GUI) in Windows. It was assigned a CVSSv3 score of 7.8 and rated as important. A local, authenticated attacker could exploit this vulnerability to elevate to SYSTEM privileges. According to Microsoft, this vulnerability was exploited in the wild as a zero-day.

CVE-2026-21525 is a denial of service (DoS) vulnerability affecting Windows Remote Access Connection Manager (also known as RasMan), a tool used for the management of multiple remote desktop connections. It was assigned a CVSSv3 score of 6.2, was rated as important and was exploited in the wild. While no information has been released about the exploitation of this DoS, the advisory credits the patch vulnerability research team for reporting this flaw.

The final actively exploited vulnerability, **CVE-2026-21533**, is a vulnerability affecting Windows Remote Desktop Services. It was assigned a CVSSv3 score of 7.8, rated as important and was reportedly exploited in the wild. Successful exploitation allows a local, authenticated attacker to elevate to SYSTEM privileges.

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 and Visual Studio
- Azure Arc
- Azure Compute Gallery
- Azure DevOps Server
- Azure Front Door (AFD)
- Azure Function
- Azure HDInsights
- Azure IoT SDK
- Azure Local
- Azure SDK
- Desktop Window Manager
- Github Copilot
- GitHub Copilot and Visual Studio
- Internet Explorer
- Mailslot File System
- Microsoft Defender for Linux
- Microsoft Edge for Android
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office Word
- Power BI
- Role: Windows Hyper-V
- Windows Ancillary Function Driver for WinSock
- Windows App for Mac
- Windows Cluster Client Failover
- Windows Connected Devices Platform Service
- Windows GDI+
- Windows HTTP.sys
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Notepad App
- Windows NTLM
- Windows Remote Access Connection Manager
- Windows Remote Desktop
- Windows Shell

- Windows Storage
- Windows Subsystem for Linux
- Windows Win32K – GRFX

Technology	Products Affected	Severity	Reference	Workaround/ Exploited / Publicly Disclosed	Vulnerability Info
Windows	Windows 10, 11 Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022, 2025 including Server Core Installations Windows App for Mac	Important	CVE-2023-2804 CVE-2026-20846 CVE-2026-21222 CVE-2026-21231 CVE-2026-21232 CVE-2026-21234 CVE-2026-21235 CVE-2026-21236 CVE-2026-21237 CVE-2026-21238 CVE-2026-21239 CVE-2026-21240 CVE-2026-21241 CVE-2026-21242 CVE-2026-21243	Workaround: No ***Exploited: Yes**** ***Public: Yes*****	Remote Code Execution Denial of Service Information Disclosure Elevation of Privilege Spoofing Security Feature Bypass

			CVE-2026-21244 CVE-2026-21245 CVE-2026-21246 CVE-2026-21247 CVE-2026-21248 CVE-2026-21249 CVE-2026-21250 CVE-2026-21251 CVE-2026-21253 CVE-2026-21255 CVE-2026-21508 ***CVE-2026-21510****,** ***CVE-2026-21513****,** CVE-2026-21517 ***CVE-2026-21519**** ***CVE-2026-21525**** ***CVE-2026-21533****		
Office	Online Server Office 2019 Excel 2016	Important	CVE-2026-21258 CVE-2026-21259	Workaround: No ***Exploited: Yes****	Information Disclosure Elevation of Privilege

	365 Apps for Enterprise LTSC 2021, 2024 (including for Mac)		CVE-2026-21260 CVE-2026-21261 CVE-2026-21511 ***CVE-2026-21514****,***	***Public: Yes****	Spoofing Security Feature Bypass
Exchange	Outlook 2016 Server Subscription Edition RTM Server 2016, 2019	Important	CVE-2026-21260 CVE-2026-21527	Workaround: No Exploited: No Public: No	Spoofing
SharePoint	Enterprise Server 2016 Server 2019 Server Subscription Edition	Important	CVE-2026-21260 CVE-2026-21511	Workaround: No Exploited: No Public: No	Spoofing
Azure	Azure Local DevOps Server 2022 Microsoft ACI Confidential Containers Azure IoT Explorer HDInsight AI Language Authoring Azure Functions Azure Front Door Azure ARC	Critical	CVE-2026-21228 CVE-2026-21512 CVE-2026-21522 CVE-2026-21528 CVE-2026-21529 CVE-2026-21531 CVE-2026-21532 CVE-2026-23655 CVE-2026-24300 CVE-2026-24302	Workaround: No Exploited: No Public: No	Remote Code Execution Spoofing Information Disclosure Elevation of Privilege

Edge	Edge (Chromium-based)	Moderate	CVE-2026-0391	Workaround: No Exploited: No Public: No	Spoofing
Notepad	Windows Notepad	Important	CVE-2026-20841	Workaround: No Exploited: No Public: No	Remote Code Execution
.Net	.NET 8.0, 9.0, 10.0	Important	CVE-2026-21218	Workaround: No Exploited: No Public: No	Spoofing
Defender	Defender for Endpoint for Linux	Important	CVE-2026-21537	Workaround: No Exploited: No Public: No	Remote Code Execution
Power BI	Power BI Report Server	Important	CVE-2026-21229	Workaround: No Exploited: No Public: No	Remote Code Execution
Developer Tools	Visual Studio 2022 version 17.14, 18.3 Visual Studio Code	Important	CVE-2026-21256 CVE-2026-21257 CVE-2026-21518 CVE-2026-21523	Workaround: No Exploited: No Public: No	Remote Code Execution Elevation of Privilege Security Feature Bypass
Other	GitHub Copilot Plugin for JetBrains IDEs	Important	CVE-2026-21516	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-february-2026-patch-tuesday-fixes-6-zero-...

https://www.tenable.com/blog/microsofts-february-2026-patch-tuesday-addresses-54-cves-cve-2026-21510-cve-2026-21513

CVE

CVE-2023-2804

CVE-2026-20846

CVE-2026-21222

CVE-2026-21231

CVE-2026-21232

CVE-2026-21234

CVE-2026-21235

CVE-2026-21236

CVE-2026-21237

CVE-2026-21238

CVE-2026-21239

CVE-2026-21240

CVE-2026-21241

CVE-2026-21242

CVE-2026-21243

CVE-2026-21244

CVE-2026-21245

CVE-2026-21246

CVE-2026-21247

CVE-2026-21248

CVE-2026-21249

CVE-2026-21250

CVE-2026-21251

CVE-2026-21253

CVE-2026-21255

CVE-2026-21508

CVE-2026-21510

CVE-2026-21513

CVE-2026-21517

CVE-2026-21519

CVE-2026-21525

CVE-2026-21533

CVE-2026-21258

CVE-2026-21259

CVE-2026-21260

CVE-2026-21261

CVE-2026-21511

CVE-2026-21514

CVE-2026-21260

CVE-2026-21527

CVE-2026-21260

CVE-2026-21511

CVE-2026-21228

CVE-2026-21512

CVE-2026-21522

CVE-2026-21528

CVE-2026-21529

CVE-2026-21531

CVE-2026-21532

CVE-2026-23655

CVE-2026-24300

CVE-2026-24302

CVE-2026-0391

CVE-2026-20841

CVE-2026-21218

CVE-2026-21229

CVE-2026-21256

CVE-2026-21257

CVE-2026-21518

CVE-2026-21523

CVE-2026-21516
CVE-2026-21537

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com