

CSIRT · ANALYSIS REPORT · UNIDEES-CSIRT-141026-001

October 2026 Patch Tuesday: analysis of 1,407 fixes and deployment priorities

UNIDEES CSIRT analysis, published 23 October 2026: exploited flaws, exploitation probabilities and recommended deployment order.

PUBLISHED
23 October 2026

VERSION
v2.0

CLASSIFICATION
Public

DATA
Microsoft as of 22 October
2026

Executive summary

- Microsoft fixed **1,407 vulnerabilities** on 13 October 2026, **77 of them critical**. Almost one in two (674) is an elevation of privilege: it does not get an attacker in, it gives them control once inside.
- **Only one flaw was exploited**: CVE-2026-96951 (Windows Shell), which removes the warning shown when opening a file from the Internet. Scored 8.8, it is not “critical” on paper, yet it is the top priority.
- **As of 23 October 2026, no other flaw is reported as exploited** (CISA catalogue 21 October 2026) and the measured exploitation probability (EPSS) does not exceed 2.9%. This time should be used to deploy.
- **54 flaws allow remote code execution with no account and no user action** (Outlook, DHCP, DNS, QUIC, Message Queuing, RRAS...). They are the easiest to exploit at scale.
- **Microsoft’s severity rating is not enough**: 61 flaws have a CVSS score of 9 or more, 47 of which are rated only “Important”.
- **Several widely used products no longer receive patches** as of this month (Windows Server 2012 and 2012 R2, Office 2021, Windows 11 24H2 Home and Pro...).

Recommended decisions

1. Deploy the CVE-2026-96951 fix to every Windows workstation and server without delay.
2. Within 72 hours, exposed servers (Exchange, AD FS, RRAS, Internet-facing services); within seven days, core infrastructure (domain controllers, DHCP, DNS, SharePoint) and Office and Outlook on every workstation.
3. List the products that reached end of support and decide, for each one, to replace or isolate it.

This month in figures

1,407

vulnerabilities fixed

77

critical according to Microsoft

1

exploited before the patch

2

publicly disclosed (1 outside Microsoft)

314

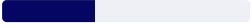
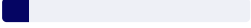
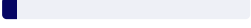
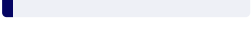
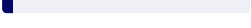
remote code execution flaws

54

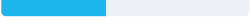
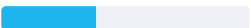
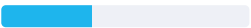
code execution with no account or user action

CSIRT calculations on Microsoft’s official data (updated 22 October 2026): CVEs published by Microsoft on 13 October 2026. We use the official source’s figures as of the data date.

BY IMPACT TYPE

Elevation of privilege		674
Remote code execution		314
Information disclosure		252
Denial of service		71
Security feature bypass		40
Tampering		29
Spoofing		27

MOST AFFECTED COMPONENTS

Microsoft Office Excel		69
Role: DNS Server		52
Windows Kernel		46
Windows Installer		38
Windows Win32 Kernel Subsystem		36
Microsoft Office SharePoint		36
Microsoft Windows Search Component		29
Windows NTFS		26
.NET		25
Microsoft Office Word		22

The volume is unusual, but the method does not change: most of the risk sits in a handful of flaws that are exploited, network-exposed or rated “exploitation more likely” by Microsoft (108 this month). Handle those first; the rest follows the normal update cycle.

What is exploited, and what is likely to be

As of 21 October 2026, the CISA Known Exploited Vulnerabilities catalogue lists only one flaw from this Patch Tuesday: **CVE-2026-96951**, added on 13 October 2026. Two flaws were made public before the patch: CVE-2026-108398 (.NET Framework, WDAC bypass) and CVE-2026-92707 (MessagePack-CSharp library, denial of service, “Moderate”, assigned by GitHub and therefore outside the scope above). The EPSS score, which estimates the probability of exploitation within 30 days, remains low for all the others: the highest is 2.9% (CVE-2026-88091). Below are the ten highest measured probabilities.

CVE	COMPONENT	IMPACT	SEVERITY	CVSS	EPSS
CVE-2026-88091	Windows Management Instrumentation	Elevation of privilege	Important	7.8	2.9%
CVE-2026-70049	Microsoft Configuration Manager	Elevation of privilege	Important	8.0	2.3%
CVE-2026-96186	Microsoft Windows Media Foundation	Elevation of privilege	Important	7.8	2.3%
CVE-2026-100214	Dynamics Business Central	Remote code execution	Important	8.8	1.8%
CVE-2026-87692	Microsoft Exchange Server	Elevation of privilege	Important	7.8	1.6%
CVE-2026-85900	Microsoft Office SharePoint	Remote code execution	Important	8.8	1.5%
CVE-2026-96951	Windows Shell	Security feature bypass	Important	8.8	1.5%
CVE-2026-70035	.NET Framework	Remote code execution	Important	8.8	1.3%
CVE-2026-83520	.NET	Remote code execution	Important	8.8	1.3%
CVE-2026-70058	Windows DHCP Server	Remote code execution	Important	7.5	1.2%

EPSS as of 22 October 2026 (FIRST). A low score is no guarantee: it changes as soon as exploit code circulates.

CSIRT priorities

Ranked by real-world risk rather than score alone: confirmed exploitation, public disclosure, unauthenticated network exposure, Microsoft’s assessment (“exploitation more likely”) and measured probability (EPSS).

-
- 01 Windows Shell: Mark of the Web bypass, exploited**
CVE-2026-96951 (important, CVSS 8.8)
The only flaw this month exploited before the patch. It removes the warning shown when opening a file from the Internet: an attacker only needs the victim to open an attachment. Added to the CISA catalogue on 13 October.
-
- 02 .NET Framework: WDAC bypass, publicly disclosed**
CVE-2026-108398 (important, CVSS 8.8)
Details were public before the patch. Allows bypassing application control (WDAC) by having a protected process load a malicious .NET assembly.
-
- 03 Outlook: five critical remote code execution flaws**
CVE-2026-70291 (critical, CVSS 9.8) · CVE-2026-70242 (critical, CVSS 9.8) · CVE-2026-97016 (critical, CVSS 9.8) · CVE-2026-88156 (critical, CVSS 9.8) · CVE-2026-97749 (critical, CVSS 9.8)
Scored 9.8, with no authentication and no user interaction according to the published vector. Outlook runs on almost every workstation.
-
- 04 Exchange Server: code execution, spoofing and elevation of privilege**
CVE-2026-70571 (critical, CVSS 8.1) · CVE-2026-70279 (important, CVSS 9.3) · CVE-2026-87692 (important, CVSS 7.8)
Microsoft rates exploitation “more likely” for the first two, the first being critical and reachable without authentication. Exchange servers are exposed by design and remain a prime target.
-
- 05 Active Directory Domain Services: critical code execution**
CVE-2026-70229 (critical, CVSS 8.1)
A crafted network packet is enough, and exploitation is rated “more likely”. Compromising a domain controller means compromising the whole environment.
-
- 06 Windows DHCP Server: critical code execution**
CVE-2026-96934 (critical, CVSS 9.8)
Scored 9.8, reachable over the network without authentication. DHCP servers exist in almost every infrastructure.
-
- 07 Microsoft QUIC: two critical code execution flaws**
CVE-2026-105016 (critical, CVSS 9.8) · CVE-2026-100219 (critical, CVSS 9.8)
Scored 9.8 without authentication. QUIC underpins HTTP/3 and SMB over QUIC: handle Internet-facing servers first.
-
- 08 Message Queuing: critical code execution**
CVE-2026-100202 (critical, CVSS 9.8)
Scored 9.8 without authentication. Check whether MSMQ is enabled: it often is without being used.
-
- 09 Word, PowerPoint, text shaping and PostScript driver**
CVE-2026-70300 (critical, CVSS 9.8) · CVE-2026-88178 (critical, CVSS 9.8) · CVE-2026-97814 (critical, CVSS 9.8) · CVE-2026-70147 (critical, CVSS 9.8) · CVE-2026-70153 (critical, CVSS 9.8)
Critical code execution, scored 9.8, in document, font and print processing. With the exploited Windows Shell flaw, booby-trapped files remain the attack vector to watch this month.
-
- 10 SharePoint: remote code execution**
CVE-2026-85900 (important, CVSS 8.8)
Among the highest measured exploitation probabilities (EPSS) this month. SharePoint often holds sensitive documents.

- 11
Dynamics 365 Business Central, WebDAV and BITS

CVE-2026-100214 (important, CVSS 8.8) · CVE-2026-102217 (important, CVSS 8.8) · CVE-2026-88159 (important, CVSS 8.8)

Exploitation rated “more likely” by Microsoft; Business Central has the highest EPSS of this month’s code execution flaws.
- 12
Elevation of privilege: WMI, Media Foundation, Configuration Manager

CVE-2026-88091 (important, CVSS 7.8) · CVE-2026-96186 (important, CVSS 7.8) · CVE-2026-70049 (important, CVSS 8.0)

The three highest exploitation probabilities (EPSS) this month; for Configuration Manager, Microsoft indicates that proof-of-concept exploit code exists. Privilege escalation turns one compromised workstation into full control.

By environment

ENVIRONMENT	FLAWS	CRITICAL	CODE EXEC.	MORE LIKELY
Active Directory and identity Domain controllers and AD FS first: one compromise is enough to take over the whole domain.	39	3	4	2
Exchange Server Exposed by design: update within 72 hours.	9	1	1	2
SharePoint High patch volume this month; Internet-facing farms first.	36	1	7	0
Office and Outlook The largest number of critical flaws: deploy to every workstation through the usual management tool.	191	35	111	0
Network services (DNS, DHCP, RRAS, RDP, IIS, SMB, QUIC...) Most flaws reachable without an account are here: start with exposed servers.	172	11	65	2
SQL Server No critical flaw, but code execution issues: include in this month's maintenance window.	23	0	9	0
.NET and Visual Studio Includes the publicly disclosed flaw; remember application servers and developer workstations.	56	0	16	0
Hyper-V and virtualisation A hypervisor flaw affects every virtual machine it hosts.	18	3	4	0
Windows kernel and drivers Mostly privilege escalation, often rated “more likely”: they serve the second stage of an attack.	299	7	22	34

End-of-support dates not to miss

- Windows Server 2012 and 2012 R2: final year of Extended Security Updates (ESU) ended on 13 October 2026.
- Windows 10 Enterprise LTSC 2016 and IoT Enterprise LTSC 2016: end of extended support.
- Office 2021, Office LTSC 2021 (Windows and Mac) and Skype for Business LTSC 2021: end of support.
- Windows 11 version 24H2 Home and Pro: last security update.
- Windows Server 2022: end of mainstream support; extended support continues until 14 October 2031.

Recommended deployment plan

Within 72 h

Exploited flaw and exposed servers

CVE-2026-96951 everywhere; Exchange, AD FS, RRAS, servers publishing QUIC or IIS to the Internet.

Within 7 days

Core infrastructure and workstations

Domain controllers, DHCP, DNS, SharePoint, Hyper-V; Office and Outlook on every workstation.

Within 30 days

The rest of the estate

Internal servers, SQL Server, .NET, developer workstations; then verify patch compliance with a vulnerability scan.

Need help prioritising or verifying your deployments?

The UNIDEES CSIRT supports organisations with prioritisation tailored to your estate, deployment follow-up, verification scans and compromise assessment. The UNIDEES CSIRT and managed SOC are ISO/IEC 27001:2022 certified. Contact: commercial@unidees.dz

Method and limitations

Scope: CVEs for which Microsoft is the assigning authority and that were published on 13 October 2026, i.e. 1,407, read from Microsoft's official data (CVRF) updated 22 October 2026. Severity: the highest rating assigned by Microsoft across affected products. Exploitation: CISA KEV catalogue (version 21 October 2026) and Microsoft indicators. Probability: EPSS as of 22 October 2026. Counts by severity and component reflect the data as of 22 October 2026. End-of-support dates are verified on Microsoft's official lifecycle site. The situation evolves: this report reflects the state as of 23 October 2026.

Sources

- Microsoft MSRC · notes de version d'octobre 2026 / October 2026 release notes
<https://msrc.microsoft.com/update-guide/releaseNote/2026-Oct>
- Microsoft MSRC · données CVRF / CVRF data
<https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Oct>
- CISA · Known Exploited Vulnerabilities
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- FIRST · EPSS
<https://www.first.org/epss/>
- Microsoft · fins de support 2026 / 2026 end of support
<https://learn.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2026>