

Alert Bulletin

Bulletin N.: 114

Publication Date: 19/10/2026

Subject: Alert 2026-114 Critical vulnerabilities in Microsoft identity, mail, and network services

Traffic Light Protocol (TLP): White

Affected product(s):

Component	CVE	CVSS	Main risk
Microsoft Outlook	CVE-2026-70242, CVE-2026-70291, CVE-2026-88156, CVE-2026-97016 and CVE-2026-97749	9.8	Remote code execution without authentication. For CVE-2026-70291 and CVE-2026-88156, the reading pane constitutes an attack vector.
Microsoft QUIC	CVE-2026-100219 and CVE-2026-105016	9.8	Remote code execution through traffic directed at services using the affected QUIC implementation.
Windows DHCP Server	CVE-2026-96934	9.8	Remote code execution through crafted packets, without credentials or user interaction.
Windows Message Queuing Queue Manager	CVE-2026-100202	9.8	Remote code execution through crafted messages sent to the MSMQ service.
Microsoft PostScript Printer Driver	CVE-2026-70147 and CVE-2026-70153	9.8	Remote code execution on affected print services, without authentication.
Microsoft Office PowerPoint	CVE-2026-88178	9.8	Code execution when processing a crafted presentation; includes preview and Office Online affected scenarios.
Active Directory Domain Services	CVE-2026-70229	8.1	Remote code execution without authentication on domain controllers; high attack complexity.
Microsoft Exchange Server	CVE-2026-70571	8.1	Remote code execution when processing crafted mail, without user interaction; high complexity.

Remote Desktop Gateway	CVE-2026-70187	8.1	Remote code execution without authentication on the gateway service; high complexity.
Windows Hyper-V	CVE-2026-102214 and CVE-2026-105733	8.8	Virtualization boundary escape from a guest machine; requires authenticated execution within the VM.

Description

Vulnerabilities of **critical** severity were published that allow remote code execution (RCE), identity spoofing, and privilege escalation in enterprise Microsoft products. The flaws in Outlook (CVE-2026-70242, CVE-2026-70291, CVE-2026-88156, CVE-2026-97016 and CVE-2026-97749), Microsoft QUIC (CVE-2026-100219 and CVE-2026-105016), DHCP Server (CVE-2026-96934), MSMQ (CVE-2026-100202) and PowerPoint (CVE-2026-88178) stand out, all with a CVSS of 9.8. Vulnerabilities in Active Directory Domain Services, Exchange Server, and Remote Desktop Gateway, with CVSS 8.1, and in Hyper-V, with CVSS 8.8, were also fixed. Several enable attacks without authentication or user interaction, so it is recommended to prioritize remediation of exposed services, identity infrastructure, and applications that process external mail or documents

The main vulnerabilities are described below:

1. Outlook and Office: compromise through crafted mail or content

The five critical Outlook vulnerabilities have a CVSS score of 9.8. In particular, CVE-2026-70291 and CVE-2026-88156 can be triggered when viewing a crafted message in the reading pane, without needing to open an attachment or click a link. This reduces the effectiveness of measures based solely on user training.

Office also presents critical flaws in PowerPoint, Word, Excel, and Visio. Among them, CVE-2026-88178 stands out due to its 9.8 score. Not all share the same vector: the critical vulnerabilities in Excel and Visio detailed by CrowdStrike do not consider the preview pane as an attack vector.

The main consequence is obtaining code execution in the context of the affected application or user, from where an attacker could attempt to access information or continue the intrusion.

• Active Directory: risk to identity infrastructure

CVE-2026-70229 allows remote code execution in Active Directory Domain Services through crafted network traffic, without authentication or interaction. Its exploitation presents high complexity and depends on configuration and timing conditions; it should not be described as a trivial compromise of any domain controller.

Two critical spoofing flaws in AD FS were also fixed:

- CVE-2026-108131 — CVSS 7.5.
- CVE-2026-96222 — CVSS 7.4; related to incorrect certificate validation.

These components require priority attention due to their role in authentication and organizational trust relationships.

- **QUIC, DHCP and MSMQ: code execution without credentials**

The QUIC, DHCP Server, and MSMQ vulnerabilities allow unauthenticated network attacks on affected services. Exposure depends on the component being installed, active, and reachable by the attacker.

In particular:

- QUIC: verify services using the affected library; it is not enough to identify only web servers.
- DHCP Server: consider accessibility from internal segments and via relays.
- MSMQ: identify dependencies of enterprise applications and exposure of TCP/1801, its usual port.

The fact that these services are not published on the Internet does not eliminate the risk: they can be targets for lateral movement from a compromised internal segment.

- **Exchange and RD Gateway: high-value exposed services**

CVE-2026-70571 affects content processing in Exchange Server and can be triggered through a specially crafted email. CVE-2026-70187 affects Remote Desktop Gateway and allows remote code execution through network traffic. Both require high-complexity exploitation conditions, but no authentication.

The assessment must distinguish RD Gateway from other Remote Desktop deployments: it is not appropriate to assume that every computer with RDP enabled presents this same scenario.

- **Hyper-V: breaking isolation between virtual machines**

CVE-2026-102214 allows an attacker with execution inside an affected VM to reach the Hyper-V host. CVE-2026-105733 is related to nested virtualization and may allow reaching the intermediate machine acting as hypervisor. They are not direct remote attacks against any host: they require prior access within the guest environment.

Exploitation status: important distinction

The vulnerability with confirmed active exploitation highlighted in the report is CVE-2026-96951, a security bypass in Windows Shell that evades Mark of the Web. Microsoft classifies it as important, not critical. It must be addressed urgently due to the evidence of attacks, even though it does not belong to the main group of this bulletin.

Confirmation of exploitation of that CVE should not be extended to the critical vulnerabilities listed above. Technical severity, public disclosure, and confirmed exploitation are different prioritization criteria.

Solution

It is recommended to apply the security updates published by Microsoft for each affected product and version, consulting the corresponding CVEs in the Microsoft Security Update Guide to identify applicable packages and requirements.

It is suggested to prioritize services exposed to the Internet, identity infrastructure, and computers that process external mail or documents; complete the required restarts and subsequently verify installed versions and remediation through a vulnerability scan. While corrections are being implemented, restricting access to affected services and disabling unnecessary components can reduce exposure, but does not replace installing the patches.

To identify affected products, requirements, packages, and corrected versions, consult the Microsoft Security Update Guide and search for each CVE:

<https://msrc.microsoft.com/security-guidance>

The MSRC portal is the official reference to determine which fix corresponds to each asset

Additional information:

- <https://msrc.microsoft.com/security-guidance>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days/>
- <https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-october-2026/>
- <https://threatprotect.qualys.com/2026/10/14/microsoft-patch-tuesday-october-2026-security-update-review/>