Microsoft Patches 1,259 Flaws, Including an Exploited Outlook Bug Tied to NTLMv2 Hash Exposure



Microsoft released fixes for 1,259 vulnerabilities, the second straight month above 1,000, including an exploited Outlook flaw that may expose NTLMv2 hashes. Prioritise the Outlook fix and plan the wider rollout.

- Microsoft patched 1,259 vulnerabilities, the second consecutive month with more than 1,000.
- The total includes 726 flaws in Windows, 174 in Office, 61 in Developer Tools, 59 in SQL Server and 27 in SharePoint Server.
- 165 of the CVE identifiers were issued by parties other than Microsoft.
- One Outlook vulnerability is reported as exploited and may expose NTLMv2 hashes.

Microsoft has released its latest security updates, covering 1,259 vulnerabilities across its products. It is the

second consecutive month in which the volume has passed 1,000 flaws.

What the release covers

Windows accounts for the largest share with 726 flaws, followed by Office with 174, Developer Tools with 61, SQL Server with 59 and SharePoint Server with 27. The release also includes 165 CVE identifiers that were not issued by Microsoft itself.

The item of most immediate concern is an Outlook vulnerability reported as exploited in the wild. It may expose NTLMv2 hashes, which are credential material that attackers can misuse in identity-based attacks. The source excerpt does not give the CVE number or further technical detail, so teams should consult Microsoft's official advisory for specifics.

What this means for your teams

A volume this large strains patch teams, so risk-based prioritisation matters. Exploited flaws and those affecting widely deployed, user-facing software such as Outlook should go first, followed by internet-facing and server products such as SharePoint Server and SQL Server.

Because the exposure concerns credential hashes, it is also a useful moment to review how NTLM is used in your environment and how far a stolen credential could travel.

What to do now

1. Identify the Outlook update for the exploited flaw in Microsoft's advisory and deploy it on an expedited schedule.
2. Prioritise remaining patches by exploitation status and exposure, starting with internet-facing and server systems.
3. Review where NTLM authentication is still in use and restrict it where business needs allow.
4. Monitor for unusual authentication activity and outbound connections that could indicate hash capture.
5. Record patch decisions and any deferrals with risk justification for audit purposes.