Microsoft Lists CVE-2026-119848, a Windows Message Queuing Denial of Service Flaw



Microsoft's update guide lists CVE-2026-119848, a denial of service vulnerability in Windows Message Queuing. The latest revision only updated an acknowledgement and does not change the guidance.

- The vulnerability is tracked as CVE-2026-119848 and affects Windows Message Queuing.
- Microsoft classifies it as a denial of service vulnerability.
- The latest revision updated an acknowledgement and is informational only.
- The source excerpt gives no severity score, affected versions or patch details.

Microsoft has published an entry in its Security Update Guide for CVE-2026-119848, described as a Windows Message Queuing Denial of Service Vulnerability. A denial of service issue, in general terms, can make a

service or system unavailable to legitimate users.

What the source says

The only change noted in the latest revision is an updated acknowledgement. Microsoft describes this as an informational change only, so it should not be read as a change to the risk or to the remediation guidance.

The excerpt available to us does not state a severity rating, the affected Windows versions, exploitation status or the specific fix. We therefore make no claims on those points.

What to do next

Security teams should review the full entry on the Microsoft Security Update Guide to confirm whether their Windows estate is affected and which update applies. Where Message Queuing is installed, it is worth knowing which servers rely on it, since availability of those systems is what this class of flaw puts at risk.

This is a routine patch-management item. Handle it through your normal change and vulnerability-management process, prioritised once the full entry confirms the scope and severity for your environment.

What to do now

1. Read the full CVE-2026-119848 entry in the Microsoft Security Update Guide to confirm affected versions and the applicable update.
2. Identify servers and applications where Windows Message Queuing is installed or in use.
3. Schedule the update through your standard change-management and patch process once scope is confirmed.
4. Record the item in your vulnerability register with its priority and remediation owner.