Health-ISAC
Collaborating for Resilience in Health

THREAT BULLETINS

POC Exploit Available for Critical WSUS Flaw CVE-2025-59287

TLP:WHITE

Oct 24, 2025

On October 23, 2025, Microsoft issued an out-of-band (OOB) security update for a critical-severity Remote Code Execution (RCE) vulnerability, tracked as CVE-2025-59287, which impacts the Windows Server Update Service (WSUS) Server Role. This threat is now categorized as urgent due to the public release of a proof-of-concept (PoC) exploit code.

The flaw tracked as CVE-2025-59287, with a CVSS score of 9.8, allows a remote, unauthorized threat actor to execute malicious code with SYSTEM privileges through a low-complexity attack requiring no user interaction. The attack vector involves sending a crafted event that triggers unsafe object deserialization in a legacy serialization mechanism. As a result of exploitation, a threat actor can take control of the WSUS Server and distribute malicious updates across managed endpoints.

The flaw was initially disclosed on October 14, 2025, and patched during October Patch Tuesday.

Only Windows servers with the optional WSUS Server Role explicitly enabled are at risk. IT administrators should prioritize the immediate deployment of the OOB security updates for all affected Windows Server versions, as this patch supersedes previous updates and requires a system reboot. If immediate patching is not possible, Microsoft suggests temporary workarounds such as disabling the WSUS Server Role to remove the attack vector or blocking all inbound traffic to Ports 8530 and 8531 on the host firewall; however, these actions will halt the delivery of updates to client endpoints.

Given the availability of the public PoC and the severity of unauthenticated SYSTEM RCE, prompt action is essential to mitigate immediate operational risk.

Sources
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

https://www.bleepingcomputer.com/news/security/microsoft-releases-windows-server-emergency-updates-for-critical-wsus-rce-flaw/

https://thecyberexpress.com/microsoft-fixes-cve-2025-59287/

https://www.helpnetsecurity.com/2025/10/24/wsus-vulnerability-cve-2025-59287-exploited/

Recommendations

- Apply OOB security patches and reboot the system.
- In cases where patching is not possible:
    1. Disable the WSUS Server Role.
    2. Block all inbound traffic to Ports 8530 and 8531.

- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Incident Date
Oct 23, 2025 (UTC)

Alert ID 1839f702

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-59287, Windows Server Update Services (WSUS)

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**