NATIONAL CSIRT CY

CVE-2025-59287: Windows Server Update Service (WSUS) Remote Code Execution Vulnerability

11/4/2025

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.

A remote, unauthenticated attacker could send a crafted event that triggers unsafe object deserialization in a legacy serialization mechanism, resulting in remote code execution.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/502.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-59287

Mitigations

Install the out-of-band update released on October 23, 2025.

Please check the **Mitigation and Workarounds** section in the vendor’s link below.

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

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.