

Date Posted: 2025/06/20

[Vulnerability Alert] Significant Security Vulnerability in Tenable's Nessus Agent (CVE-2025-36633)

- Subject: [Vulnerability Alert] Significant Security Vulnerability in Tenable's Nessus Agent (CVE-2025-36633)
- Content Description:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202506-00000015
 - Tenable provides the widely deployed vulnerability scanning tool Nessus and the world's first exposure management platform to view and maintain the security of digital assets on any platform. Recently, Tenable issued a significant security announcement (CVE-2025-36633, CVSS: 8.8). This vulnerability, in Nessus Agent versions prior to 10.8.5 (exclusive) on Windows hosts, allows non-administrator users to arbitrarily delete local system files with SYSTEM privileges, leading to local privilege escalation.
- Affected Platforms:
 - Tenable Agent 10.8.5 (exclusive) and earlier versions
- Suggested Measures:
 - Please update to Tenable Agent 10.8.5
- References:
 - <https://www.twcert.org.tw/tw/cp-169-10191-409d1-1.html>

Computer and Communications Center
Network Systems Division Respectfully

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250620_02



Last update: **2025/06/20 15:40**