

Posted Date: 2025/08/25

[Vulnerability Alert] CISA Added 5 Known Exploited Vulnerabilities to KEV Catalog (2025/08/11-2025/08/17)

- Subject: [Vulnerability Alert] CISA Added 5 Known Exploited Vulnerabilities to KEV Catalog (2025/08/11-2025/08/17)
- Content:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202508-00000012
 - 1. [CVE-2025-8088] RARLAB WinRAR Path Traversal Vulnerability (CVSS v3.1: 8.8)
 - [Exploited by ransomware: Unknown] RARLAB WinRAR has a path traversal vulnerability that affects its Windows version. Attackers can execute arbitrary code by creating a malicious compressed file.
 - [Affected Platforms] Please refer to the affected versions listed by the official source
 - <https://www.win-rar.com/>
 - 2. [CVE-2007-0671] Microsoft Office Excel Remote Code Execution Vulnerability (CVSS v3.1: 8.8)
 - [Exploited by ransomware: Unknown] Microsoft Office Excel has a remote code execution vulnerability. An attacker can execute remote code on the affected system by using a specially crafted Excel file.
 - [Affected Platforms] Please refer to the affected versions listed by the official source
 - <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2007/ms07-015>
 - 3. [CVE-2013-3893] Microsoft Internet Explorer Resource Management Errors Vulnerability (CVSS v3.1: 8.8)
 - [Exploited by ransomware: Unknown] Microsoft Internet Explorer has a memory corruption vulnerability that could lead to remote code execution.
 - [Affected Platforms] Please refer to the affected versions listed by the official source
 - <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-080>
 - 4. [CVE-2025-8876] N-able N-Central Command Injection Vulnerability (CVSS v3.1: 8.8)
 - [Exploited by ransomware: Unknown] N-able N-Central has a command injection vulnerability due to improper filtering of user input.
 - [Affected Platforms] Please refer to the affected versions listed by the official source
 - <https://status.n-able.com/2025/08/13/announcing-the-ga-of-n-central-2025-3-1/>
 - 5. [CVE-2025-8875] N-able N-Central Insecure Deserialization Vulnerability (CVSS v3.1: 7.8)
 - [Exploited by ransomware: Unknown] N-able N-Central has an insecure deserialization vulnerability that could lead to command execution.
 - [Affected Platforms] Please refer to the affected versions listed by the official source
 - <https://status.n-able.com/2025/08/13/announcing-the-ga-of-n-central-2025-3-1/>
- Affected Platforms:
 - Please refer to the Affected Platforms section in the content description.
- Recommended Measures:
 1. [CVE-2025-8088] The official source has released a patch for the vulnerability; please update to the relevant version.
 - <https://www.win-rar.com/>
 2. [CVE-2007-0671] The official source has released a patch for the vulnerability; please

update to the relevant version.

- <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2007/ms07-015>
- 3. [CVE-2013-3893] The official source has released a patch for the vulnerability; please update to the relevant version.
 - <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-080>
- 4. [CVE-2025-8876] The official source has released a patch for the vulnerability; please update to the relevant version.
 - <https://status.n-able.com/2025/08/13/announcing-the-ga-of-n-central-2025-3-1/>
- 5. [CVE-2025-8875] The official source has released a patch for the vulnerability; please update to the relevant version.
 - <https://status.n-able.com/2025/08/13/announcing-the-ga-of-n-central-2025-3-1/>

Computer and Communications Center
Network Systems Group

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250825_01 

Last update: **2025/08/25 16:51**