

Date 2025/05/16

[Vulnerability Alert] NetWeaver has a security vulnerability (CVE-2025-31324), please confirm and fix it as soon as possible

- Subject Description: [Vulnerability Alert] NetWeaver has a security vulnerability (CVE-2025-31324), please confirm and fix it as soon as possible
- Content Description:
 - Forwarded by National Cyber Security Information Sharing and Analysis Center NISAC-200-202505-00000027
 - Researchers have discovered an arbitrary file upload vulnerability (CVE-2025-31324) in the Visual Composer Metadata Uploader component of NetWeaver, allowing unauthenticated remote attackers to exploit this vulnerability to upload and execute malicious programs. This vulnerability has been exploited by hackers, please confirm and fix it as soon as possible.
- Affected Platforms:
 - NetWeaver 7.x versions
- Recommended Actions:
 - Versions 7.5 and above have released patches SP027 - SP033, it is recommended to install the patches
 - Versions 7.4 and below are recommended to be updated to version 7.5 and above and install patches or take mitigation measures
 - The official has released patch and mitigation instructions, the URLs are as follows (login required):
 1. <https://me.sap.com/notes/3594142>
 2. <https://me.sap.com/notes/3596125/E>
 3. <https://me.sap.com/notes/3593336/E>
- References:
 1. <https://nvd.nist.gov/vuln/detail/CVE-2025-31324>
 2. <https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/>
 3. <https://securitybridge.com/blog/cve-2025-31324>
 4. <https://techcommunity.microsoft.com/blog/microsoftdefendercloudblog/guidance-for-handling-cve-2025-31324-using-microsoft-security-capabilities/4409413>
 5. https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html?anchorId=section_370125364

Network System Division
Computer and Communication Center9

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250516_01 

Last update: **2025/05/16 16:26**