N-Partner

Security Bulletin 2025

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2025/09/01

We are committed to closely monitoring information security issues and have implemented patches for known vulnerabilities. Detailed information has been compiled in the table below, which includes descriptions of security issues, remediation methods, affected products, updated versions, and severity levels. This table will provide a clear overview of the security measures implemented, ensuring you have a comprehensive understanding of our security strategy.

Updated Date	PSIRT	Description	Affected Products	Solution	Severity
Jul 14, 2025	NP-IR-25-0701	Patch Vulnerability: CVE-2025-49812, CVE-2025-53020, CVE-2025-23048, CVE-2024-43394, CVE-2024-42516, CVE-2025-27363 Upgrade: Apache to 2.4.62, Freetype to 2.13.3-1	N-Cloud 7.0.02X, N-Reporter 7.0.02X	Upgrade to Kernel 20250714123258 or above	Medium
Apr 21, 2025	NP-IR-25-0401	Upgrade: PHP OpenSSL extension to support TLS version 1.3	N-Cloud 7.0.02X, N-Reporter 7.0.02X	Upgrade to Kernel 20250421224704, Image 20250421 or above	Medium
Feb 26, 2025	NP-IR-25-0202	Patch Vulnerability: CVE-2024-3596 Blast RADIUS	N-Cloud 7.0.02X, N-Reporter 7.0.02X	Upgrade to Kernel 20250226230815 or above	Medium
Feb 25, 2025	NP-IR-25-0201	Patch Vulnerability: CVE-2025-26466, CVE-2025-26465 Upgrade: OpenSSH version to 9.9p2	N-Cloud 7.0.02X, N-Reporter 7.0.02X	Upgrade to Kernel 20250225013851 or above	Medium

We strongly recommend that all users refer to the above solutions and update their systems immediately. This version addresses the identified vulnerabilities, helping to mitigate associated risks. For technical support or to report additional security issues, please contact our security team:

Email: support@npartner.com

Phone: 04-23752865 #9

Tel：04-23752865
Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com