N-Partner

Security Bulletin 2026

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2026/01/12

N-Partner is committed to closely monitoring information security issues and has implemented patches for known vulnerabilities. Detailed information has been compiled in the table below, which includes descriptions of security issues (with CVE ID), remediation methods, affected products, updated versions, and severity levels (refer to Common Vulnerability Scoring System，CVSS). This table provides a clear overview of the security measures implemented, ensuring a comprehensive understanding of N-Partner’s security strategy.

Updated Date	PSIRT	Description	Affected Products	Solution	Severity
Jan 12, 2026	NP-IR-26-0101	Patch Vulnerability: CVE-2025-61984 Upgrade: OpenSSH to 10.2p1	N-Cloud 6.1.X, N-Cloud 7.0.X, N-Reporter 6.1.X, N-Reporter 7.0.X, N-Probe 6.X, N-Probe 7.0.X	Kernel Upgrade: 20251216135658 Download	Low

N-Partner strongly recommends that all users refer to the above solutions and update their systems immediately. This version addresses the identified vulnerabilities, helping to mitigate associated risks.
Please refer to the documentation: How to Update N-Reporter/N-Cloud Firmware and Kernel
For version 7.X and above, you can also refer to the N-Partner YouTube channel: How to Upgrade Device Firmware and Kernel

For technical support or to report additional security issues, please contact the N-Partner 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

N-Reporter N-Cloud N-Probe N-Robot