



CVE-2008-2369

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2008-2369
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-14 20:41:00 UTC
Updated	2022-02-03 19:57:00 UTC
Description	manzier.pxt in Red Hat Network Satellite Server before 5.1.1 has a hard-coded authentication key, which allows remote att

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Satellite	All	All	All	All
Application	Red Hat	Network Satellite Server	2	All	All	All
Application	Red Hat	Network Satellite Server	2.0.1	All	All	All
Application	Red Hat	Network Satellite Server	2.6	All	All	All
Application	Red Hat	Network Satellite Server	2.7	All	All	All
Application	Red Hat	Network Satellite Server	3	All	All	All
Application	Red Hat	Network Satellite Server	3.2	All	All	All
Application	Red Hat	Network Satellite Server	3.4	All	All	All
Application	Red Hat	Network Satellite Server	3.6	All	All	All
Application	Red Hat	Network Satellite Server	3.7	All	All	All
Application	Red Hat	Network Satellite Server	3.7.2	All	All	All
Application	Red Hat	Network Satellite Server	4	All	All	All
Application	Red Hat	Network Satellite Server	4.0.1	All	All	All
Application	Red Hat	Network Satellite Server	4.0.2	All	All	All
Application	Red Hat	Network Satellite Server	4.0.5	All	All	All
Application	Red Hat	Network Satellite Server	4.0.6	All	All	All
Application	Red Hat	Network Satellite Server	4.0.7	All	All	All

Application	Red Hat	Network Satellite Server	4.1	All	All	All
Application	Red Hat	Network Satellite Server	4.1.2	All	All	All
Application	Red Hat	Network Satellite Server	4.1.5	All	All	All
Application	Red Hat	Network Satellite Server	4.2	All	All	All
Application	Red Hat	Network Satellite Server	4.2.1	All	All	All
Application	Red Hat	Network Satellite Server	4.2.2	All	All	All
Application	Red Hat	Network Satellite Server	5	All	All	All
Application	Red Hat	Network Satellite Server	5.0.1	All	All	All
Application	Red Hat	Network Satellite Server	5.1.0	All	All	All
Application	Red Hat	Network Satellite Server	2	All	All	All
Application	Red Hat	Network Satellite Server	2.0.1	All	All	All
Application	Red Hat	Network Satellite Server	2.6	All	All	All
Application	Red Hat	Network Satellite Server	2.7	All	All	All
Application	Red Hat	Network Satellite Server	3	All	All	All
Application	Red Hat	Network Satellite Server	3.2	All	All	All
Application	Red Hat	Network Satellite Server	3.4	All	All	All
Application	Red Hat	Network Satellite Server	3.6	All	All	All
Application	Red Hat	Network Satellite Server	3.7	All	All	All
Application	Red Hat	Network Satellite Server	3.7.2	All	All	All
Application	Red Hat	Network Satellite Server	4	All	All	All
Application	Red Hat	Network Satellite Server	4.0.1	All	All	All
Application	Red Hat	Network Satellite Server	4.0.2	All	All	All
Application	Red Hat	Network Satellite Server	4.0.5	All	All	All
Application	Red Hat	Network Satellite Server	4.0.6	All	All	All
Application	Red Hat	Network Satellite Server	4.0.7	All	All	All
Application	Red Hat	Network Satellite Server	4.1	All	All	All
Application	Red Hat	Network Satellite Server	4.1.2	All	All	All
Application	Red Hat	Network Satellite Server	4.1.5	All	All	All
Application	Red Hat	Network Satellite Server	4.2	All	All	All
Application	Red Hat	Network Satellite Server	4.2.1	All	All	All
Application	Red Hat	Network Satellite Server	4.2.2	All	All	All
Application	Red Hat	Network Satellite Server	5	All	All	All
Application	Red Hat	Network Satellite Server	5.0.1	All	All	All
Application	Red Hat	Network Satellite Server	5.1.0	All	All	All

References

Reference

SecurityTracker.com Archives - Red Hat Network Satellite Server 'manzier.pxt' Hard Coded Common Authentication Key Lets Remote Users C

Red Hat Network Satellite Server 'manzier.pxt' User Information Disclosure Vulnerability

IBM X-Force Exchange

Red Hat update for Red Hat Network Satellite Server - Secunia Advisories - Vulnerability Intelligence - Secunia.com

access.redhat.com

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)