



CVE-2013-1841

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

Summary

CVE	CVE-2013-1841
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-13 14:55:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	Net-Server, when the reverse-lookups option is enabled, does not check if the hostname resolves to the source IP address.

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Seamons	Net-server	-	All	All	All
Application	Seamons	Net-server	-	All	All	All

References

Reference	Source	L
oss-security - Re: Reverse lookup issue in Net::Server	MLIST	w
Net-Server 'allow_deny()' Function Security Bypass Vulnerability	BID	w
oss-security - Reverse lookup issue in Net::Server	MLIST	w
920683 – (CVE-2013-1841) CVE-2013-1841 perl-Net-Server: Improper reverse DNS matching check for the given hostname	CONFIRM	b
IBM X-Force Exchange	XF	e
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[753797](#) SUSE Enterprise Linux Security Update for perl-Net-Server (SUSE-SU-2023:0746-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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