



CVE-2020-35513

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

Summary

CVE	CVE-2020-35513
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	A flaw incorrect umask during file or directory modification in the Linux kernel NFS (network file system) functionality was fo

Risk And Classification

Problem Types: CWE-271

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	4.2	All	All	All
Operating System	Linux	Linux Kernel	4.2	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source	Link
nfsd: zero out umask if the client didn't provide one - Patchwork		patchwork
1911309 – (CVE-2020-35513) CVE-2020-35513 kernel: Nfsd failure to clear umask after processing an open or create	MISC	bugzilla
nfsd: zero out umask if the client didn't provide one - Patchwork	MISC	patchwork
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nis

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](#).

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

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