



CVE-2018-18955

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

Summary

CVE	CVE-2018-18955
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-16 20:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In the Linux kernel 4.15.x through 4.19.x before 4.19.2, map_write() in kernel/user_namespace.c allows privilege escalation

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
1712 - Linux: broken uid/gid mapping for nested user namespaces with >5 ranges - project-zero - Monorail	MISC	bugs.chromium.org
USN-3832-1: Linux kernel (AWS) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
support.f5.com/csp/article/K39103040	CONFIRM	support.f5.com
USN-3835-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
Linux - Nested User Namespace idmap Limit Local Privilege Escalation (Metasploit) - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com

cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.18.19	MISC	cdn.kernel.org
CVE-2018-18955 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.2	MISC	cdn.kernel.org
users: also map extents in the reverse map to kernel IDs · torvalds/linux@d2f007d · GitHub	MISC	github.com
USN-3836-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Linux - Broken uid/gid Mapping for Nested User Namespaces - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
USN-3836-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3833-1: Linux kernel (AWS) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Linux Kernel CVE-2018-18955 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)