CVE-2016-9604

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-9604
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-11 13:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, such as '.dns_re

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	4.11	rc1	All	All
Operating System	Linux	Linux Kernel	4.11	rc2	All	All
Operating System	Linux	Linux Kernel	4.11	rc3	All	All
Operating System	Linux	Linux Kernel	4.11	rc4	All	All
Operating System	Linux	Linux Kernel	4.11	rc5	All	All
Operating System	Linux	Linux Kernel	4.11	rc6	All	All
Operating System	Linux	Linux Kernel	4.11	rc7	All	All
Operating System	Linux	Linux Kernel	4.11	rc1	All	All
Operating System	Linux	Linux Kernel	4.11	rc2	All	All
Operating System	Linux	Linux Kernel	4.11	rc3	All	All
Operating System	Linux	Linux Kernel	4.11	rc4	All	All
Operating System	Linux	Linux Kernel	4.11	rc5	All	All
Operating System	Linux	Linux Kernel	4.11	rc6	All	All
Operating System	Linux	Linux Kernel	4.11	rc7	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
Red Hat Customer Portal
1389433 – (CVE-2016-9604) CVE-2016-9604 kernel: security: The built-in keyrings for security tokens can be joined as a session and then m
Red Hat Customer Portal
Linux Kernel 'security/keys/keyctl.c' Local Security Bypass Vulnerability
CVE-2016-9604 in Ubuntu
kernel/git/torvalds/linux.git - Linux kernel source tree
Bug 1035576 – VUL-0: CVE-2016-9604: kernel-source: Keyrings whose name begin with a '.' are special internal keyrings and souserspace is
Red Hat Customer Portal
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**