



CVE-2018-14634

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

Summary

CVE	CVE-2018-14634
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-25 21:29:00 UTC
Updated	2023-02-13 04:51:00 UTC
Description	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access

Risk And Classification

EPSS: 0.223610000 probability, percentile 0.957830000 (date 2026-04-01)

CISA KEV: Listed on 2026-01-26; due 2026-02-16; ransomware use Unknown

Problem Types: CWE-190

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Integer Overflow Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/about/ ; https://www.kernel.org/ ; https://www.cve.org/CVERecord?id=CVE-2018-14634 ; https://access.redhat.com/errata/RHSA-2018:3540 ; https://nvd.nist.gov/vuln/detail/CVE-2018-14634

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Active Iq Performance Analytics Services	-	All	All	All
Application	Netapp	Active Iq Performance Analytics Services	-	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference

Red Hat Customer Portal

support.f5.com/csp/article/K20934447

Red Hat Customer Portal

Red Hat Customer Portal

1624498 – (CVE-2018-14634) CVE-2018-14634 kernel: Integer overflow in Linux's create_elf_tables function

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

CVE-2018-14634 Linux Kernel Integer Overflow Vulnerability in NetApp Products | NetApp Product Security

Red Hat Customer Portal

Red Hat Customer Portal

1624498 – (CVE-2018-14634) CVE-2018-14634 kernel: Integer overflow in Linux's create_elf_tables function

oss-security - Integer overflow in Linux's create_elf_tables() (CVE-2018-14634)

USN-3775-1: Linux kernel vulnerabilities | Ubuntu security notices

oss-security - CVE-2021-33910: Denial of service (stack exhaustion) in systemd (PID 1)

USN-3779-1: Linux kernel vulnerabilities | Ubuntu security notices

CVE-2018-14634 Privilege Escalation in PAN-OS

Red Hat Customer Portal

Linux Kernel 'create_elf_tables()' Function Local Integer Overflow Vulnerability

USN-3775-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices

support.f5.com/csp/article/K20934447

Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - 'Mutagen Astronomy' Local Privilege Escalation - Linux_x86-64 local E

Red Hat Customer Portal

Red Hat Customer Portal

CVE-2018-14634 - Red Hat Customer Portal

Mutagen Astronomy - Local privilege escalation - CVE-2018-14634 - Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

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

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](#)