

CVE-2014-0196

Linux Kernel Race Condition Vulnerability

CISA KEV since May 12, 2023

Actively exploited

The `n_tty_write` function in `drivers/tty/n_tty.c` in the Linux kernel through 3.14.3 does not properly manage tty driver access in the "LECHO & !OPOST" case, which allows local users to cause a denial of service (memory corruption and system crash) or gain privileges by triggering a race condition involving read and write operations with long strings.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.5 Medium · NVD	EPSS 0.203 97.5th percentile · FIRST	CISA DEADLINE Jun 2, 2023 KEV since 2023 · listed over a year
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.203 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: The impacted product is end-of-life and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions · 22 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip access policy manager	≥ 11.1.0 ≤ 11.5.1	no fixed version listed	NVD
big-ip advanced firewall manager	≥ 11.3.0 ≤ 11.5.1	no fixed version listed	NVD
big-ip analytics	≥ 11.1.0 ≤ 11.5.1	no fixed version listed	NVD
big-ip application acceleration manager	≥ 11.4.0 ≤ 11.5.1	no fixed version listed	NVD
big-ip application security manager	≥ 11.1.0 ≤ 11.5.1	no fixed version listed	NVD
big-ip edge gateway	≥ 11.1.0 ≤ 11.3.0	no fixed version listed	NVD
big-ip global traffic manager	≥ 11.1.0 ≤ 11.5.1	no fixed version listed	NVD
big-ip link controller	≥ 11.1.0 ≤ 11.5.1	no fixed version listed	NVD

Sources

Vendor guidance bugzilla.redhat.com/show_bug.cgi?id=1094232

lkml.iu.edu lkml.iu.edu/hypermail/linux/kernel/1609.1/02103.html

NVD nvd.nist.gov/vuln/detail/CVE-2014-0196

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2014-0247

Current data evulnable.com/vulnerability-management/cve/CVE-2014-0196

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.