

CVE-2017-1000253

Linux Kernel PIE Stack Buffer Corruption Vulnerability

CISA KEV since Sep 9, 2024

Actively exploited

Ransomware use known

Linux distributions that have not patched their long-term kernels with <https://git.kernel.org/linus/a87938b2e246b81b4fb713edb371a9fa3c5c3c86> (committed on April 14, 2015). This kernel vulnerability was fixed in April 2015 by commit [a87938b2e246b81b4fb713edb371a9fa3c5c3c86](https://git.kernel.org/linus/a87938b2e246b81b4fb713edb371a9fa3c5c3c86) (backported to Linux 3.10.77 in May 2015), but it was not recognized as a security threat.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.107 95.8th percentile · FIRST	CISA DEADLINE Sep 30, 2024 KEV since 2024 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.107 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.
Basis: CISA KEV required action

With CONFIG_ARCH_BINFORMAT_ELF_RANDOMIZE_PIE enabled, and a normal top-down address allocation strategy, `load_elf_binary()` will attempt to map a PIE binary into an address range immediately below `mm->mmap_base`. Unfortunately, `load_elf_binary()` does not take account of the need to allocate sufficient space for the entire binary which means that, while the first PT_LOAD segment is mapped below `mm->mmap_base`, the subsequent PT_LOAD segment(s) end up being mapped above `mm->mmap_base` into the area that is supposed to be the "gap" between the stack and the binary.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
centos	6.0	no fixed version listed	NVD
	6.1		
	6.2		
	6.3		
	6.4		
	6.5		
	6.6		
	6.7		
	6.8		
	6.9		
	7.1406		
	7.1503		
	7.1511		
	7.1611		
enterprise linux	6.0	no fixed version listed	NVD
	6.1		
	6.2		
	6.3		
	6.4		
	6.5		
	6.6		
	6.7		
	6.8		
	6.9		
	7.0		
	7.1		
	7.2		
	7.3		
linux kernel	≥ 2.6.25 < 3.2.70	no fixed version listed	NVD
	≥ 3.3 < 3.4.109		
	≥ 3.5 < 3.10.77		
	≥ 3.11 < 3.12.43		
	≥ 3.13 < 3.14.41		
	≥ 3.15 < 3.16.35		
	≥ 3.17 < 3.18.14		
	≥ 3.19 < 3.19.7		
	≥ 4.0 < 4.0.2		

Sources

Vendor guidance	qualys.com/2017/09/26/cve-2017-1000253/cve-2017-1000253.txt	Additional guidance	access.redhat.com/errata/RHSA-2017:2798
git.kernel.org	git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=a87938b2e246b81b4fb713edb371a9fa3c5c3c86	NVD	nvd.nist.gov/vuln/detail/CVE-2017-1000253
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-1514
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-1000253		

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