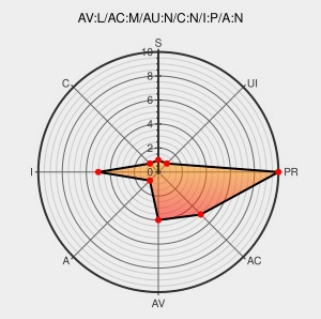
CVE-2013-1958

Published on: 04/24/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:42:00 AM UTC

CVE-2013-1958

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The scm_check_creds function in net/core/scm.c in the Linux kernel before 3.8.6 does not properly enforce capability requirements for controlling the PID value associated with a UNIX domain socket, which allows local users to bypass intended access restrictions by leveraging the time interval during which a user namespace has been created but a PID namespace has not been created.

CVE-2013-1958 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
scm: Require CAP_SYS_ADMIN over the current pidns to spoof pids. · torvalds/linux@92f28d9 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/92f28d973cce45ef5823209aab3138eb45d8b349
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.8.6
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=92f28d973cce45ef5823209aab3138eb45d8b349

	Inactive Link Not Archived	
oss-security - Re: Re: Summary of security bugs (now fixed) in user namespaces	www.openwall.com text/html	MLIST [oss-security] 20130416 Re: Re: Summary of security bugs (now fixed) in user namespaces

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.3	All	All	All
Operating System	Linux	Linux Kernel	3.8.4	All	All	All
Operating System	Linux	Linux Kernel	3.8.0	All	All	All
Operating System	Linux	Linux Kernel	3.8.1	All	All	All
Operating System	Linux	Linux Kernel	3.8.2	All	All	All
Operating System	Linux	Linux Kernel	3.8.3	All	All	All
Operating System	Linux	Linux Kernel	3.8.4	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.8.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→