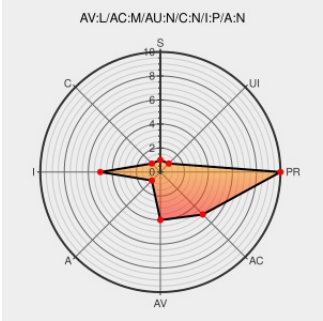
CVE-2012-1568

Published on: 02/28/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:33:00 AM UTC

CVE-2012-1568

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The ExecShield feature in a certain Red Hat patch for the Linux kernel in Red Hat Enterprise Linux (RHEL) 5 and 6 and Fedora 15 and 16 does not properly handle use of many shared libraries by a 32-bit executable file, which makes it easier for context-dependent attackers to bypass the ASLR protection mechanism by leveraging a predictable base address for one of these libraries.

CVE-2012-1568 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
Security: Some random observations on Linux ASLR	scarybeastsecurity.blogspot.com, text/html	MISC scarybeastsecurity.blogspot.com/2012/03/some-random-observations-on-linux-aslr.html
804947 – (CVE-2012-1568) CVE-2012-1568 kernel: execshield: predictable ascii armour base address	bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=804947
oss-security - Re: CVE request	openwall.com	MLIST [oss-security] 20120321 Re: CVE request -- kernel: execshield: predictable ascii armour base address

CVE request -- kernel: execshield: predictable ascii armour base address	text/html	predictable ascii armour base address
oss.oracle.com - redpatch.git/commit	web.archive.org text/xml Inactive Link Not Archived	MISC oss.oracle.com/git/?p=redpatch.git%3Ba=commit%3Bh=302a4fc15aebf202b6dffd6c804377c6058ee6e4
oss-security - Re: CVE request -- kernel: execshield: predictable ascii armour base address	www.openwall.com text/html	MLIST [oss-security] 20120320 Re: CVE request -- kernel: execshield: predictable ascii armour base address

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

cpe:2.3:o:fedoraproject:fedora:15:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:16:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:15:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:16:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→