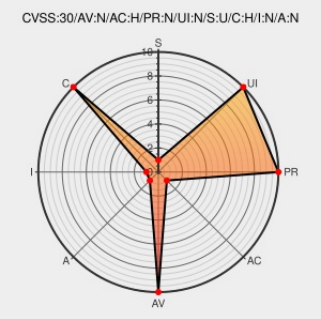
CVE-2011-4190

Published on: 06/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

CVE-2011-4190

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



Certain versions of Suse Linux Enterprise Desktop from Suse contain the following vulnerability:

The kdump implementation is missing the host key verification in the kdump and mkdumprd OpenSSH integration of kdump prior to version 2012-01-20. This is similar to CVE-2011-3588, but different in that the kdump implementation is specific to SUSE. A remote malicious kdump server could use this flaw to impersonate the correct kdump server to obtain security sensitive information (kdump core files).

CVE-2011-4190 has been assigned by security@microfocus.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SUSE** - **kdump** version **2012-01-20**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link

Bug 722440 – VUL-1: kexec-tools: Multiple security flaws by management of kdump core files and ramdisk images	Issue Tracking bugzilla.suse.com text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=722440
CVE-2011-4190 | SUSE	Vendor Advisory www.suse.com text/html	CONFIRM www.suse.com/security/cve/CVE-2011-4190/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11.0	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	11.0	sp1	All	All

cpe:2.3:o:suse:suse_linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:sap_aio:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11.0:sp1:*:*:ltss:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:sap_aio:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11.0:sp1:*:*:ltss:*:*:*:

Discovery Credit

Discovery Credit

Kevan Carstensen

← Previous ID

Next ID→