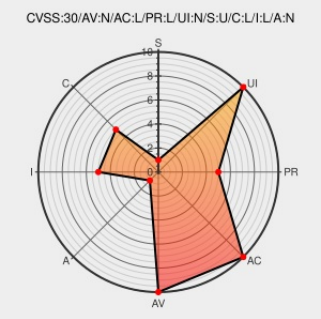
CVE-2011-3172

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

Last Modified on: 03/23/2021 11:23:14 PM UTC

CVE-2011-3172

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



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

A vulnerability in pam_modules of SUSE Linux Enterprise allows attackers to log into accounts that should have been disabled. Affected releases are SUSE Linux Enterprise: versions prior to 12.

CVE-2011-3172 has been assigned by ot security@microfocus.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: ot **SUSE** - **SUSE Linux Enterprise** version **12**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bug 707645 – VUL-1: CVE-2011-3172: pam: unix2_chkpwd do not check for a valid account	Issue Tracking, bugzilla.suse.com, text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=707645

Request 80346 - openSUSE Build Service	Vendor Advisory build.opensuse.org text/html	CONFIRM build.opensuse.org/request/show/80346

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 Server	All	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	All	All	All	All

cpe:2.3:o:suse:suse_linux_enterprise_server:*:*:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:*:*:*:*:*:*:*:*:

Discovery Credit

Michael Calmer of SUSE

← Previous ID

Next ID→