CVE-2002-1160

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2002-1160
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-02-19 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The default configuration of the pam_xauth module forwards MIT-Magic-Cookies to new X sessions, which could allow loca

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Linux	7.1	All	All	All

Operating System	Redhat	Linux	7.2	All	All	All
Operating System	Redhat	Linux	7.3	All	All	All
Operating System	Redhat	Linux	8.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
redhat.com | Red Hat Support	af854a
redhat.com | Red Hat Support	af854a
ISS X-Force Database: linux-pamxauth-gain-privileges (11254): Red Hat Linux pam_xauth could allow an attacker to gain privileges	af854a
'BDT_AV200212140001: Insecure default: Using pam_xauth for su from sh-utils package' - MARC	af854a
PAM pam_xauth Module Unintended X Session Cookie Access Vulnerability	af854a
Free Sun Alert Notifications Article 55760	af854a
Mandrakesoft Security Advisories	af854a
CERT/CC Vulnerability Note VU#911505	af854a
Home - Conectiva	af854a
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.