CVE-2011-2520

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

Summary

CVE	CVE-2011-2520
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-21 23:55:00 UTC
Updated	2024-01-21 02:53:00 UTC
Description	fw_dbus.py in system-config-firewall 1.2.29 and earlier uses the pickle Python module unsafely during D-Bus communicatio

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	15	All	All	All
Application	Redhat	System-config-firewall	1.2.11	All	All	All
Application	Redhat	System-config-firewall	1.2.12	All	All	All
Application	Redhat	System-config-firewall	1.2.14	All	All	All
Application	Redhat	System-config-firewall	1.2.15	All	All	All
Application	Redhat	System-config-firewall	1.2.16	All	All	All
Application	Redhat	System-config-firewall	1.2.17	All	All	All
Application	Redhat	System-config-firewall	1.2.21	All	All	All
Application	Redhat	System-config-firewall	1.2.22	All	All	All
Application	Redhat	System-config-firewall	1.2.23	All	All	All
Application	Redhat	System-config-firewall	1.2.24	All	All	All
Application	Redhat	System-config-firewall	1.2.25	All	All	All
Application	Redhat	System-config-firewall	1.2.26	All	All	All
Application	Redhat	System-config-firewall	1.2.27	All	All	All
Application	Redhat	System-config-firewall	1.2.28	All	All	All
Application	Redhat	System-config-firewall	1.2.11	All	All	All
Application	Redhat	System-config-firewall	1.2.12	All	All	All

Application	Redhat	System-config-firewall	1.2.14	All	All	All
Application	Redhat	System-config-firewall	1.2.15	All	All	All
Application	Redhat	System-config-firewall	1.2.16	All	All	All
Application	Redhat	System-config-firewall	1.2.17	All	All	All
Application	Redhat	System-config-firewall	1.2.21	All	All	All
Application	Redhat	System-config-firewall	1.2.22	All	All	All
Application	Redhat	System-config-firewall	1.2.23	All	All	All
Application	Redhat	System-config-firewall	1.2.24	All	All	All
Application	Redhat	System-config-firewall	1.2.25	All	All	All
Application	Redhat	System-config-firewall	1.2.26	All	All	All
Application	Redhat	System-config-firewall	1.2.27	All	All	All
Application	Redhat	System-config-firewall	1.2.28	All	All	All
Application	Redhat	System-config-firewall	All	All	All	All

References

Reference	Source	Link
Support	REDHAT	www.redhat.com
Red Hat update for system-config-firewall - Secunia.com	SECUNIA	secunia.com
Bug 717985 – CVE-2011-2520 system-config-firewall: privilege escalation flaw via use of python pickle	CONFIRM	bugzilla.redhat.com
Red Hat Customer Portal	MISC	access.redhat.com
SecurityTracker: Red Hat system-config-firewall Lets Local Users Gain Root Privileges	SECTRACK	securitytracker.com
IBM X-Force Exchange	XF	exchange.xforce.ibr
CVE-2011-2520 - Red Hat Customer Portal	MISC	access.redhat.com
[SECURITY] Fedora 15 Update: system-config-firewall-1.2.29-4.fc15	FEDORA	lists.fedoraproject.o
Red Hat system-config-firewall Local Privilege Escalation Vulnerability	BID	www.securityfocus.(
oss-security - CVE-2011-2520: flaw in system-config-firewall's usage of pickle allows privilege escalation	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report