



CVE-2007-6131

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2007-6131
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-11-26 22:46:00 UTC
Updated	2011-03-08 03:01:00 UTC
Description	buttonpressed.sh in scanbuttond 0.2.3 allows local users to overwrite arbitrary files via a symlink attack on the (1) scan.pnr

Risk And Classification

Problem Types: CWE-16

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Fedora Core	f7	All	All	All
Operating System	Redhat	Fedora Core	f7	All	All	All

References

Reference	Source	Link
scanbuttond Insecure Temporary File Creation Vulnerability	BID	www.securityfocus.com
42422	OSVDB	osvdb.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Bug 383131 – CVE-2007-6131 scanbuttond: unsafe usage of temporary files in buttonpressed.sh	CONFIRM	bugzilla.redhat.com
Fedora scanbuttond Insecure Temporary Files - Advisories - Secunia	SECUNIA	secunia.com
scanbuttond Symlink Bug Lets Local Users Gain Root Privileges - SecurityTracker	SECTRACK	securitytracker.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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)