



CVE-2011-3211

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-3211
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-16 12:35:00 UTC
Updated	2011-09-23 03:34:00 UTC
Description	The server in Bcfg2 1.1.2 and earlier, and 1.2 prerelease, allows remote attackers to execute arbitrary commands via shell

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bcfg2	Bcfg2	0.3.1	All	All	All
Application	Bcfg2	Bcfg2	0.4	All	All	All
Application	Bcfg2	Bcfg2	0.5	All	All	All
Application	Bcfg2	Bcfg2	0.6	All	All	All
Application	Bcfg2	Bcfg2	0.6.1	All	All	All
Application	Bcfg2	Bcfg2	0.6.10	All	All	All
Application	Bcfg2	Bcfg2	0.6.3	All	All	All
Application	Bcfg2	Bcfg2	0.6.4	All	All	All
Application	Bcfg2	Bcfg2	0.6.5	All	All	All
Application	Bcfg2	Bcfg2	0.6.6	All	All	All
Application	Bcfg2	Bcfg2	0.6.7	All	All	All
Application	Bcfg2	Bcfg2	0.6.8	All	All	All
Application	Bcfg2	Bcfg2	0.6.9	All	All	All
Application	Bcfg2	Bcfg2	0.7.0	All	All	All
Application	Bcfg2	Bcfg2	0.7.1	All	All	All
Application	Bcfg2	Bcfg2	0.7.2	All	All	All
Application	Bcfg2	Bcfg2	0.7.3	All	All	All

Application	Bcfg2	Bcfg2	0.7.4	All	All	All
Application	Bcfg2	Bcfg2	0.8.0	All	All	All
Application	Bcfg2	Bcfg2	0.8.1	All	All	All
Application	Bcfg2	Bcfg2	0.8.2	All	All	All
Application	Bcfg2	Bcfg2	0.8.3	All	All	All
Application	Bcfg2	Bcfg2	0.8.4	All	All	All
Application	Bcfg2	Bcfg2	0.8.5	All	All	All
Application	Bcfg2	Bcfg2	0.8.6.1	All	All	All
Application	Bcfg2	Bcfg2	0.8.7	All	All	All
Application	Bcfg2	Bcfg2	0.8.7.1	All	All	All
Application	Bcfg2	Bcfg2	0.8.7.2	All	All	All
Application	Bcfg2	Bcfg2	0.9.0	All	All	All
Application	Bcfg2	Bcfg2	0.9.1d	All	All	All
Application	Bcfg2	Bcfg2	0.9.2	All	All	All
Application	Bcfg2	Bcfg2	0.9.3	All	All	All
Application	Bcfg2	Bcfg2	0.9.4	All	All	All
Application	Bcfg2	Bcfg2	0.9.5	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.1	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.2	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.3	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.5	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.7	All	All	All
Application	Bcfg2	Bcfg2	0.9.6	All	All	All
Application	Bcfg2	Bcfg2	1.0	pre1	All	All
Application	Bcfg2	Bcfg2	1.0	pre2	All	All
Application	Bcfg2	Bcfg2	1.0	pre4	All	All
Application	Bcfg2	Bcfg2	1.0.0	All	All	All
Application	Bcfg2	Bcfg2	1.0.1	All	All	All
Application	Bcfg2	Bcfg2	1.1.0	All	All	All
Application	Bcfg2	Bcfg2	1.1.1	All	All	All
Application	Bcfg2	Bcfg2	1.2	prerelease	All	All
Application	Bcfg2	Bcfg2	0.3.1	All	All	All
Application	Bcfg2	Bcfg2	0.4	All	All	All
Application	Bcfg2	Bcfg2	0.5	All	All	All
Application	Bcfg2	Bcfg2	0.6	All	All	All

Application	Bcfg2	Bcfg2	0.6.1	All	All	All
Application	Bcfg2	Bcfg2	0.6.10	All	All	All
Application	Bcfg2	Bcfg2	0.6.3	All	All	All
Application	Bcfg2	Bcfg2	0.6.4	All	All	All
Application	Bcfg2	Bcfg2	0.6.5	All	All	All
Application	Bcfg2	Bcfg2	0.6.6	All	All	All
Application	Bcfg2	Bcfg2	0.6.7	All	All	All
Application	Bcfg2	Bcfg2	0.6.8	All	All	All
Application	Bcfg2	Bcfg2	0.6.9	All	All	All
Application	Bcfg2	Bcfg2	0.7.0	All	All	All
Application	Bcfg2	Bcfg2	0.7.1	All	All	All
Application	Bcfg2	Bcfg2	0.7.2	All	All	All
Application	Bcfg2	Bcfg2	0.7.3	All	All	All
Application	Bcfg2	Bcfg2	0.7.4	All	All	All
Application	Bcfg2	Bcfg2	0.8.0	All	All	All
Application	Bcfg2	Bcfg2	0.8.1	All	All	All
Application	Bcfg2	Bcfg2	0.8.2	All	All	All
Application	Bcfg2	Bcfg2	0.8.3	All	All	All
Application	Bcfg2	Bcfg2	0.8.4	All	All	All
Application	Bcfg2	Bcfg2	0.8.5	All	All	All
Application	Bcfg2	Bcfg2	0.8.6.1	All	All	All
Application	Bcfg2	Bcfg2	0.8.7	All	All	All
Application	Bcfg2	Bcfg2	0.8.7.1	All	All	All
Application	Bcfg2	Bcfg2	0.8.7.2	All	All	All
Application	Bcfg2	Bcfg2	0.9.0	All	All	All
Application	Bcfg2	Bcfg2	0.9.1d	All	All	All
Application	Bcfg2	Bcfg2	0.9.2	All	All	All
Application	Bcfg2	Bcfg2	0.9.3	All	All	All
Application	Bcfg2	Bcfg2	0.9.4	All	All	All
Application	Bcfg2	Bcfg2	0.9.5	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.1	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.2	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.3	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.5	All	All	All
Application	Bcfg2	Bcfg2	0.9.5.7	All	All	All
Application	Bcfg2	Bcfg2	0.9.6	All	All	All

Application	Bcfg2	Bcfg2	0.9.6	All	All	All
Application	Bcfg2	Bcfg2	1.0	pre1	All	All
Application	Bcfg2	Bcfg2	1.0	pre2	All	All
Application	Bcfg2	Bcfg2	1.0	pre4	All	All
Application	Bcfg2	Bcfg2	1.0.0	All	All	All
Application	Bcfg2	Bcfg2	1.0.1	All	All	All
Application	Bcfg2	Bcfg2	1.1.0	All	All	All
Application	Bcfg2	Bcfg2	1.1.1	All	All	All
Application	Bcfg2	Bcfg2	1.2	prerelease	All	All
Application	Bcfg2	Bcfg2	All	All	All	All

References
Reference
Security Advisory SA46042 - Fedora update for bcfg2 - Secunia
[SECURITY] Fedora 14 Update: bcfg2-1.1.2-2.fc14
Bug 736279 – CVE-2011-3211 bcfg2 (bcfg2-server): Privilege escalation due to improper escaping of shell command data sent from client, w
Bcfg2 Remote Command Injection Vulnerability
article.gmane.org 522: Connection timed out
#640028 - Unescaped shell command vulnerabilities - Debian Bug report logs
bcfg2 Command Injection Vulnerabilities - Secunia.com
fixed security bugs with unescaped input to the shell · solj/bcfg2@f4a35ef · GitHub
oss-security - CVE request for bcfg2 (remote root)
oss-security - Re: CVE request for bcfg2 (remote root)
Backported unescaped shell command fixes from master branch · solj/bcfg2@46795ae · GitHub
Debian -- Security Information -- DSA-2302-1 bcfg2
Debian update for bcfg2 - Secunia.com
[SECURITY] Fedora 15 Update: bcfg2-1.1.2-2.fc15
CVE Program record
NVD vulnerability detail
◀
▶

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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