



CVE-2009-3369

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

Summary

CVE	CVE-2009-3369
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-24 16:30:00 UTC
Updated	2009-10-31 06:22:00 UTC
Description	CgiUserConfigEdit in BackupPC 3.1.0, when SSH keys and Rsync are in use in a multi-user environment, does not restrict

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Craig Barratt	Backuppc	3.1.0	All	All	All
Application	Craig Barratt	Backuppc	3.1.0	All	All	All

References

Reference	Source
Fedora update for BackupPC - Secunia.com	SECUNIA
Bug 518412 – CVE-2009-3369 BackupPC: Permission bypass via ClientNameAlias by using rsync data backup method	CONFIR
57236	OSVDB
[SECURITY] Fedora 10 Update: BackupPC-3.1.0-6.fc10	FEDORA
BackupPC "ClientNameAlias" SSH Rsync Backup Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
#542218 - backuppc: Security hole when using rsync and multiple users - Debian Bug report logs	MISC
[SECURITY] Fedora 11 Update: BackupPC-3.1.0-7.fc11	FEDORA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

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