

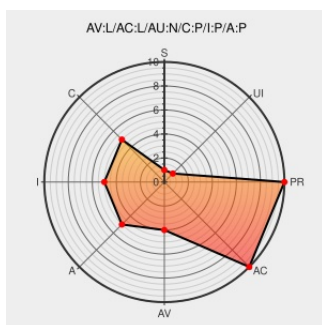


CVE-2006-1390

Published on: 03/24/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1390

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux](#) from [Gentoo](#) contain the following vulnerability:

The configuration of NetHack 3.4.3-r1 and earlier, Falcon's Eye 1.9.4a and earlier, and Slash'EM 0.0.760 and earlier on Gentoo Linux allows local users in the games group to modify saved games files to execute arbitrary code via buffer overflows and overwrite arbitrary files via symlink attacks.

CVE-2006-1390 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060324 Re: \[GLSA 200603-23 \] NetHack, Slash'EM, Falcon's Eye: Local privilege escalation](#)

127319 – games-roguelike/falconseye: local privilege escalation

bugs.gentoo.org
text/html

[MISC bugs.gentoo.org/show_bug.cgi?id=127319](http://misc.bugs.gentoo.org/show_bug.cgi?id=127319)

122376 – games-roguelike/nethack: insecure save game creation

Exploit
bugs.gentoo.org
text/html

[MISC bugs.gentoo.org/show_bug.cgi?id=122376](http://misc.bugs.gentoo.org/show_bug.cgi?id=122376)

127167 – games-roguelike/slashem: insecure save game creation and local priv escalation(CVE-2006-1390)

bugs.gentoo.org
text/html

[MISC bugs.gentoo.org/show_bug.cgi?id=127167](http://misc.bugs.gentoo.org/show_bug.cgi?id=127167)

SecurityFocus

www.securityfocus.com

[BUGTRAQ 20060324 Re: \[GLSA 200603-23 \] NetHack, Slash'EM, Falcon's Eye: Local privilege escalation](#)

	text/html	200603-23 J NetHack, Slash'EM, Falcon's Eye: Localprivilege escalation
Gentoo Nethack And Variants Local Privilege Escalation Vulnerability	cve.report (archive) text/html	 BID 17217
Gentoo Linux Documentation -- NetHack, Slash'EM, Falcon's Eye: Local privilege escalation	Patch www.gentoo.org text/html	 GENTOO GLSA-200603-23
Gentoo Bug 125902 - games-roguelike/nethack: local privilege escalation and insecure savegame creation (CVE-2006-1390)	Exploit bugs.gentoo.org text/html	 MISC bugs.gentoo.org/show_bug.cgi?id=125902
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF gentoo-multiple-games-privilege-escalation(25528)
Gentoo nethack / falconseye / slashem Privilege Escalation - Advisories - Secunia	Vendor Advisory web.archive.org text/html	 SECUNIA 19376
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 24104

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	0.5	All	All	All
Operating System	Gentoo	Linux	0.7	All	All	All
Operating System	Gentoo	Linux	1.1a	All	All	All
Operating System	Gentoo	Linux	1.2	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	rc1	All	All
Operating System	Gentoo	Linux	1.4	rc2	All	All
Operating System	Gentoo	Linux	1.4	rc3	All	All
Operating System	Gentoo	Linux	0.5	All	All	All
Operating System	Gentoo	Linux	0.7	All	All	All

Operating System	Gentoo	Linux	1.1a	All	All	All
Operating System	Gentoo	Linux	1.2	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	rc1	All	All
Operating System	Gentoo	Linux	1.4	rc2	All	All
Operating System	Gentoo	Linux	1.4	rc3	All	All
cpe:2.3:o:gentoo:linux:0.5:*****:						
cpe:2.3:o:gentoo:linux:0.7:*****:						
cpe:2.3:o:gentoo:linux:1.1a:*****:						
cpe:2.3:o:gentoo:linux:1.2:*****:						
cpe:2.3:o:gentoo:linux:1.4:*****:						
cpe:2.3:o:gentoo:linux:1.4:rc1:*****:						
cpe:2.3:o:gentoo:linux:1.4:rc2:*****:						
cpe:2.3:o:gentoo:linux:1.4:rc3:*****:						
cpe:2.3:o:gentoo:linux:0.5:*****:						
cpe:2.3:o:gentoo:linux:0.7:*****:						
cpe:2.3:o:gentoo:linux:1.1a:*****:						
cpe:2.3:o:gentoo:linux:1.2:*****:						
cpe:2.3:o:gentoo:linux:1.4:*****:						
cpe:2.3:o:gentoo:linux:1.4:rc1:*****:						
cpe:2.3:o:gentoo:linux:1.4:rc2:*****:						
cpe:2.3:o:gentoo:linux:1.4:rc3:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)