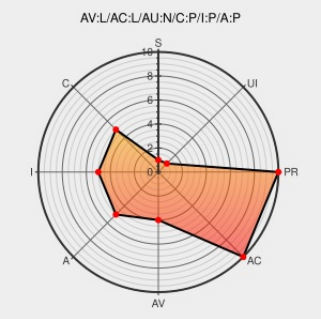
CVE-2006-1390

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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
122376 – games-roguelike/nethack: insecure save game creation	Exploit bugs.gentoo.org text/html	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
SecurityFocus	www.securityfocus.com	BUGTRAQ 20060324 Re: [GLSA

	text/html	200603-23] 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

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→

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