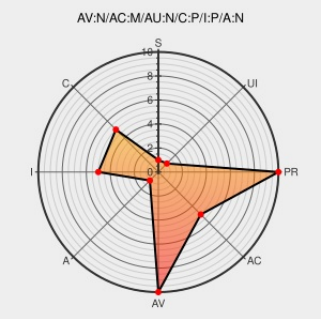
CVE-2011-4093

Published on: 02/10/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:21:00 AM UTC

CVE-2011-4093

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Net6 from Armin Burgmeier contain the following vulnerability:

Integer overflow in inc/server.hpp in libnet6 (aka net6) before 1.3.14 might allow remote attackers to hijack connections and gain privileges as other users by making a large number of connections until the overflow occurs and an ID of another user is provided.

CVE-2011-4093 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
openSUSE-SU-2012:0040-1: moderate: net6	Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2012:0040
openSUSE-SU-2012:0008-1: moderate: net6	Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2012:0008
git.0x539.de Git - net6.git/commitdiff	Patch, git.0x539.de, text/xml	MISC git.0x539.de/?p=net6.git%3Ba=commitdiff%3Bh=ac61d7fb42a1f977fb527e024bede319c4a9e169%3Bhp=(
Bug 727710 – VUL-0: net6 connection hijacking	Issue Tracking, Third Party Advisory, VDB Entry, bugzilla.novell.com, text/html	CONFIRM bugzilla.novell.com/show_bug.cgi?id=727710

750631 – (CVE-2011-4093) CVE-2011-4093 net6: integer overflow may lead to connection hijacking	Issue Tracking Third Party Advisory VDB Entry bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=750631
oss-security - Re: CVE request: 3 flaws in libobby and libnet6	Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20111031 Re: CVE request: 3 flaws in libobby and libnet6
Oracle Solaris Third Party Bulletin - April 2015	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2015-2511959.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Armin Burgmeier	Net6	1.3.1	All	All	All
Application	Armin Burgmeier	Net6	1.3.10	All	All	All
Application	Armin Burgmeier	Net6	1.3.11	All	All	All
Application	Armin Burgmeier	Net6	1.3.12	All	All	All
Application	Armin Burgmeier	Net6	1.3.2	All	All	All
Application	Armin Burgmeier	Net6	1.3.3	All	All	All
Application	Armin Burgmeier	Net6	1.3.4	All	All	All
Application	Armin Burgmeier	Net6	1.3.5	All	All	All
Application	Armin Burgmeier	Net6	1.3.6	All	All	All
Application	Armin Burgmeier	Net6	1.3.7	All	All	All
Application	Armin Burgmeier	Net6	1.3.8	All	All	All
Application	Armin Burgmeier	Net6	1.3.9	All	All	All
Application	Armin Burgmeier	Net6	1.3.1	All	All	All
Application	Armin Burgmeier	Net6	1.3.10	All	All	All
Application	Armin Burgmeier	Net6	1.3.11	All	All	All
Application	Armin Burgmeier	Net6	1.3.12	All	All	All
Application	Armin Burgmeier	Net6	1.3.2	All	All	All

Application	Armin Burgmeier	Net6	1.3.3	All	All	All
Application	Armin Burgmeier	Net6	1.3.4	All	All	All
Application	Armin Burgmeier	Net6	1.3.5	All	All	All
Application	Armin Burgmeier	Net6	1.3.6	All	All	All
Application	Armin Burgmeier	Net6	1.3.7	All	All	All
Application	Armin Burgmeier	Net6	1.3.8	All	All	All
Application	Armin Burgmeier	Net6	1.3.9	All	All	All
Application	Armin Burgmeier	Net6	All	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse Project	Opensuse	11.4	All	All	All
Operating System	Opensuse Project	Opensuse	11.4	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All

cpe:2.3:a:armin_burgmeier:net6:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.12:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.12:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:1.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:armin_burgmeier:net6:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse_project:opensuse:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse_project:opensuse:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:oracle:solaris:11.2:*:*:*:*:*:*:*:

cpe:2.3:o:oracle:solaris:11.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→