



# CVE-2014-3468

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

## Summary

<b>CVE</b>	CVE-2014-3468
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-06-05 20:55:00 UTC
<b>Updated</b>	2020-11-16 14:30:00 UTC
<b>Description</b>	The asn1_get_bit_der function in GNU Libtasn1 before 3.6 does not properly report an error when a negative bit length is ic

## Risk And Classification

**Problem Types:** CWE-131

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Hardware	F5	Arx	-	All	All	All
Hardware	F5	Arx	-	All	All	All
Operating System	F5	Arx Firmware	All	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Application	Gnu	Libtasn1	All	All	All	All
Application	Gnu	Libtasn1	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All



Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Virtualization	6.0	All	All	All
Application	Redhat	Virtualization	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp3	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All

## References

Reference	Source	Link
linux.oracle.com   ELSA-2014-0594 - gnutls security update	CONFIRM	<a href="http://linux.oracle.com">linux.oracle.com</a>
Security Advisory SA61888 - Debian update for libtasn1-3 - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Security Advisory SA58614 - Red Hat update for libtasn1 - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
support.f5.com/kb/en-us/solutions/public/15000/400/sol15423.html	CONFIRM	<a href="http://support.f5.com">support.f5.com</a>
Debian -- Security Information -- DSA-3056-1 libtasn1-3	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
www.novell.com/support/kb/doc.php	CONFIRM	<a href="http://www.novell.com">www.novell.com</a>
About Secunia Research   Flexera	SECUNIA	<a href="http://secunia.com">secunia.com</a>
About Secunia Research   Flexera	SECUNIA	<a href="http://secunia.com">secunia.com</a>
www.novell.com/support/kb/doc.php	CONFIRM	<a href="http://www.novell.com">www.novell.com</a>
libtasn1.git - GNU libtasn1	CONFIRM	<a href="http://git.savannah.gnu.or">git.savannah.gnu.or</a>
Security Advisory SA59408 - Novell Open Enterprise Server GnuTLS Multiple Vulnerabilities - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Security Advisory SA59021 - Oracle Linux update for gnutls - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>

About Secunia Research   Flexera	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Security Advisory SA58591 - Oracle Linux update for libtasn1 - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
linux.oracle.com   ELSA-2014-0596 - libtasn1 security update	CONFIRM	<a href="http://linux.oracle.com">linux.oracle.com</a>
1102323 – (CVE-2014-3468) CVE-2014-3468 libtasn1: asn1_get_bit_der() can return negative bit length	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
GNU Libtasn1 3.6 released	MLIST	<a href="http://lists.gnu.org">lists.gnu.org</a>
Support / Security / Advisories // MDVSA-2015:116   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Mageia Advisory: MGASA-2014-0247 - Updated libtasn1 packages fix CVE-2014-3467-9	CONFIRM	<a href="http://advisories.mageia.org">advisories.mageia.org</a>
[security-announce] SUSE-SU-2014:0788-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
[security-announce] SUSE-SU-2014:0758-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

900178 CBL-Mariner Linux Security Update for gnutls 3.6.14

© 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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)