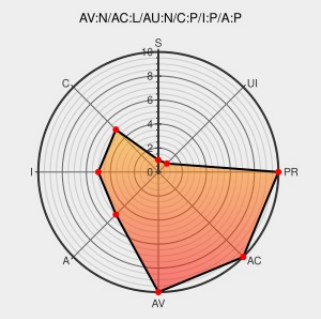
CVE-2005-1600

Published on: 05/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

CVE-2005-1600

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



Certain versions of Libtomcrypt from Libtomcrypt contain the following vulnerability:

A "mathematical flaw" in the implementation of the El Gamal signature algorithm for LibTomCrypt 1.0 to 1.0.2 allows attackers to generate valid signatures without having the private key.

CVE-2005-1600 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Secunia - Advisories - LibTomCrypt ECC Signature Scheme Vulnerability	web.archive.org text/html	SECUNIA 15233
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF libtomcrypt-signature-security-bypass(20455)
LibTomCrypt El Gamal Implementation Flaw Valid Signature Generation Vulnerability	cve.report (archive) text/html	BID 13473
No Description Provided	www.securityfocus.org Inactive Link Not Archived	BUGTRAQ 20050503 Secure Science Corporation Advisory CSA-056
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 16188

SecuriTeam.com ™ - LibTomCrypt Weak Signature Scheme	www.securiteam.com text/html	MISC www.securiteam.com/unixfocus/5JP092AFPG.html

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
Application	Libtomcrypt	Libtomcrypt	1.0	All	All	All
Application	Libtomcrypt	Libtomcrypt	1.0.1	All	All	All
Application	Libtomcrypt	Libtomcrypt	1.0.2	All	All	All
Application	Libtomcrypt	Libtomcrypt	1.0	All	All	All
Application	Libtomcrypt	Libtomcrypt	1.0.1	All	All	All
Application	Libtomcrypt	Libtomcrypt	1.0.2	All	All	All

cpe:2.3:a:libtomcrypt:libtomcrypt:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtomcrypt:libtomcrypt:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:libtomcrypt:libtomcrypt:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:libtomcrypt:libtomcrypt:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:libtomcrypt:libtomcrypt:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:libtomcrypt:libtomcrypt:1.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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