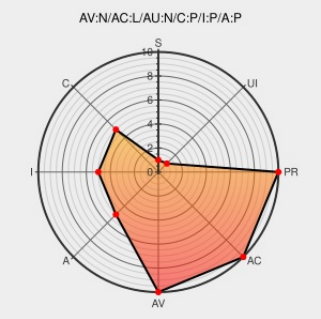
CVE-2007-2232

Published on: 04/25/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:42 PM UTC

CVE-2007-2232

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



Certain versions of Cosign from Cosign contain the following vulnerability:

The CHECK command in Cosign 2.0.1 and earlier allows remote attackers to bypass authentication requirements via CR (\r) sequences in the cosign cookie parameter.

CVE-2007-2232 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
	Vendor Advisory, www.umich.edu, text/plain	CONFIRM www.umich.edu/~umweb/software/cosign/cosign-vuln-2007-001.txt
SecurityFocus	web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20070411 Cosign SSO Authentication Bypass
CoSign POST Request Carriage Return Insertion Vulnerabilities - Advisories - Secunia	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 24845
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2007-1359

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	Cosign	Cosign	0.7.0	All	All	All
Application	Cosign	Cosign	0.8.0	All	All	All
Application	Cosign	Cosign	0.9.0	All	All	All
Application	Cosign	Cosign	1.0	All	All	All
Application	Cosign	Cosign	1.1	All	All	All
Application	Cosign	Cosign	1.5	All	All	All
Application	Cosign	Cosign	1.6	All	All	All
Application	Cosign	Cosign	1.7	All	All	All
Application	Cosign	Cosign	1.8	All	All	All
Application	Cosign	Cosign	1.8.5	All	All	All
Application	Cosign	Cosign	1.9	All	All	All
Application	Cosign	Cosign	2.0.1	All	All	All
Application	Cosign	Cosign	0.7.0	All	All	All
Application	Cosign	Cosign	0.8.0	All	All	All
Application	Cosign	Cosign	0.9.0	All	All	All
Application	Cosign	Cosign	1.0	All	All	All
Application	Cosign	Cosign	1.1	All	All	All
Application	Cosign	Cosign	1.5	All	All	All
Application	Cosign	Cosign	1.6	All	All	All
Application	Cosign	Cosign	1.7	All	All	All
Application	Cosign	Cosign	1.8	All	All	All
Application	Cosign	Cosign	1.8.5	All	All	All
Application	Cosign	Cosign	1.9	All	All	All
Application	Cosign	Cosign	2.0.1	All	All	All

cpe:2.3:a:cosign:cosign:0.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:0.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:0.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.7:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.8:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.9:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:0.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:0.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:0.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.7:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.8:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:1.9:*:*:*:*:*:*:*:

cpe:2.3:a:cosign:cosign:2.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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