



CVE-2011-1332

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

Summary

CVE	CVE-2011-1332
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-29 17:55:00 UTC
Updated	2011-06-29 17:55:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Cybozu Garoon 2.0.0 through 2.1.3 allows remote attackers to inject arbitrary web

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cybozu	Garoon	2.0.0	All	All	All
Application	Cybozu	Garoon	2.0.1	All	All	All
Application	Cybozu	Garoon	2.0.2	All	All	All
Application	Cybozu	Garoon	2.0.3	All	All	All
Application	Cybozu	Garoon	2.0.4	All	All	All
Application	Cybozu	Garoon	2.0.5	All	All	All
Application	Cybozu	Garoon	2.0.6	All	All	All
Application	Cybozu	Garoon	2.1.0	All	All	All
Application	Cybozu	Garoon	2.1.1	All	All	All
Application	Cybozu	Garoon	2.1.2	All	All	All
Application	Cybozu	Garoon	2.1.3	All	All	All
Application	Cybozu	Garoon	2.0.0	All	All	All
Application	Cybozu	Garoon	2.0.1	All	All	All
Application	Cybozu	Garoon	2.0.2	All	All	All
Application	Cybozu	Garoon	2.0.3	All	All	All
Application	Cybozu	Garoon	2.0.4	All	All	All
Application	Cybozu	Garoon	2.0.5	All	All	All

Application	Cybozu	Garoon	2.0.6	All	All	All
Application	Cybozu	Garoon	2.1.0	All	All	All
Application	Cybozu	Garoon	2.1.1	All	All	All
Application	Cybozu	Garoon	2.1.2	All	All	All
Application	Cybozu	Garoon	2.1.3	All	All	All

References			
Reference	Source	Link	Tags
JVNDB-2011-000044	JVNDB	jvndb.jvn.jp	
お探しのページが見つかりませんでした。 サイボウズ株式会社	CONFIRM	cybozu.co.jp	Patch, Vendor Advisory
JVN#59779256: Cybozu Garoon vulnerable to cross-site scripting	JVN	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.