CVE-2008-3102

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-3102
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-09-24 11:42:00 UTC
Updated	2018-10-11 20:45:00 UTC
Description	Mantis 1.1.x through 1.1.2 and 1.2.x through 1.2.0a2 does not set the secure flag for the session cookie in an https session

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mantisbt	Mantisbt	1.1.0	All	All	All
Application	Mantisbt	Mantisbt	1.1.1	All	All	All
Application	Mantisbt	Mantisbt	1.1.2	All	All	All
Application	Mantisbt	Mantisbt	1.2.0a1	All	All	All
Application	Mantisbt	Mantisbt	1.2.0a2	All	All	All
Application	Mantisbt	Mantisbt	1.1.0	All	All	All
Application	Mantisbt	Mantisbt	1.1.1	All	All	All
Application	Mantisbt	Mantisbt	1.1.2	All	All	All
Application	Mantisbt	Mantisbt	1.2.0a1	All	All	All
Application	Mantisbt	Mantisbt	1.2.0a2	All	All	All

References

Reference	Source
Gentoo update for mantisbt - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
[SECURITY] Fedora 8 Update: mantis-1.1.4-1.fc8	FEDORA
SecurityFocus	BUGTRAC

[SECURITY] Fedora 9 Update: mantis-1.1.4-1.fc9	FEDORA
Fedora update for mantis - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Mantis: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO
Mantis: Session hijacking vulnerability, CVE-2008-3102	MISC
SecurityFocus	BUGTRAC
Mantis Referenced Reports Information Disclosure Security Issue - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Mantis Insecure Cookie Disclosure Weakness	BID
SecurityReason - menalto gallery: Session hijacking vulnerability	SREASON
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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