CVE-2007-1681

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

Summary

CVE	CVE-2007-1681
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-19 10:19:00 UTC
Updated	2018-10-16 16:40:00 UTC
Description	Format string vulnerability in libwebconsole_services.so in Sun Java Web Console 2.2.2 through 2.2.5 allows remote attack

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sun	Java Web Console	2.2.2	All	x86	All
Application	Sun	Java Web Console	2.2.3	All	x86	All
Application	Sun	Java Web Console	2.2.4	All	x86	All
Application	Sun	Java Web Console	2.2.5	All	x86	All
Application	Sun	Java Web Console	2.2.2	All	x86	All
Application	Sun	Java Web Console	2.2.3	All	x86	All
Application	Sun	Java Web Console	2.2.4	All	x86	All
Application	Sun	Java Web Console	2.2.5	All	x86	All
Operating System	Sun	Solaris	10.0	All	x86	All
Operating System	Sun	Solaris	10.0	hw2	All	All
Operating System	Sun	Solaris	10.0	All	x86	All
Operating System	Sun	Solaris	10.0	hw2	All	All

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Sun Solaris and Java Web Console Format String Vulnerability - Advisories - Secunia	SECUNIA

#102854: Security Vulnerability in the Sun Java Web Console May Allow Access to Privileged Data or Lead to Denial of Service	SUNALERT
34902	OSVDB
SecurityFocus	BUGTRAQ
Repository / Oval Repository	OVAL
IBM X-Force Exchange	XF
n.runs AG - Security Tools and Security Advisories	MISC
Sun Java Web Console LibWebconsole_Services.SO Format String Vulnerability	BID
Sun Java Web Console Format String Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK
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**