



CVE-2008-3869

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

Summary

CVE	CVE-2008-3869
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-05-26 21:30:00 UTC
Updated	2018-10-11 20:50:00 UTC
Description	Heap-based buffer overflow in sadmind in Sun Solaris 8 and 9 allows remote attackers to execute arbitrary code via a crafted

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sun	Solaris	8.0	All	sparc	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All
Operating System	Sun	Solaris	8.0	All	sparc	All
Operating System	Sun	Solaris	8.0	All	x86	All
Operating System	Sun	Solaris	9.0	All	sparc	All
Operating System	Sun	Solaris	9.0	All	x86	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vu
Avaya CMS Solaris "sadmind" Two Vulnerabilities - Secunia.com	SECUNIA	secunia
SecurityFocus	BUGTRAQ	www.se
Vulnerabilities - Secunia Research - Vulnerability Information - Secunia.com	MISC	secunia
Repository / Oval Repository	OVAL	oval.cis
Sun Solaris "sadmind" Two Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia

Sun Solaris 'sadmind' Daemon Multiple Buffer Overflow Vulnerabilities	BID	www.se
sunsolve.sun.com/search/document.do	CONFIRM	sunsolv
ASA-2009-195 (SUN 259468)	CONFIRM	support.
54663	OSVDB	www.os
SecurityTracker.com Archives - sadmind Buffer Overflows Let Remote Users Execute Arbitrary Code	SECTrack	www.se
#259468: Multiple Vulnerabilities in the Solaris 8 and 9 sadmind(1M) Daemon May Lead to Arbitrary Code Execution	SUNALERT	sunsolv
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist



No vendor comments have been submitted for this CVE.

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