



CVE-2006-3968

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

Summary

CVE	CVE-2006-3968
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-01 22:04:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	The crypto provider in Sun Solaris 10 3/05 HW2 without patch 121236-01, when running on Sun Fire T2000 platforms, incor

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sun	Solaris	10.0	hw2	All	All
Operating System	Sun	Solaris	10.0	hw2	All	All

References

Reference	Source	Link
102543	SUNALERT	sunsolve
Sun Fire T2000 Incorrect DSA Signature Verification - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vuln
IBM X-Force Exchange	XF	exchang
Sun Fire T2000 Incorrect DSA Signature Verification Vulnerability	BID	www.sec
SecurityTracker.com Archives - Sun Fire T2000 Does Not Properly Detect Invalid DSA Signatures	SECTRACK	securityt
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)