



CVE-2006-7140

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

Summary

CVE	CVE-2006-7140
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-07 20:19:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	The libike library, as used by in.iked, elfsign, and kcfd in Sun Solaris 9 and 10, when using an RSA key with exponent 3, re

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
Operating System	Sun	Sunos	5.9	All	All	All
Operating System	Sun	Sunos	5.9	All	All	All

References

Reference	Source	Link
#201390: Security Vulnerability With RSA Signature Affects Solaris Applications Utilizing the libike Library	SUNALERT	sunsolve.sun.com
Sun Solaris libike RSA Signature Forgery - Advisories - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
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](#).

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