



CVE-2000-0704

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

Summary	
CVE	CVE-2000-0704
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-10-20 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in SGI Omron WorldView Wnn allows remote attackers to execute arbitrary commands via long JS_OPEN,

Risk And Classification	
Primary CVSS:	v2.0 10 from nvd@nist.gov
AV:N/AC:L/Au:N/C:C/I:C/A:C	
Problem Types:	NVD-CWE-Other n/a

CVSS v2.0 Breakdown	
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Complete
Integrity	Complete
Availability	Complete
AV:N/AC:L/Au:N/C:C/I:C/A:C	

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Freewnn	Freewnn	1.0	All	All	All

Application	Freewnn	Freewnn	1.1	All	All	All
Application	Freewnn	Freewnn	1.1.1_axxx	All	All	All
Application	Omron	Worldview	6.5	All	All	All
Application	Wnn	Wnn4	4.2.2tl	All	All	All
Application	Wnn	Wnn4	4.2.5tl	All	All	All
Application	Wnn	Wnn4	4.2.8	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References		
Reference	Source	Link
www.osvdb.org/11080	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org/11080
Omron WorldView Wnn Asian Language Server Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secmirror.com/2020/08/04/omron-worldview-wnn-asian-language-server-remote-buffer-overflow-vulnerability/
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com/af854a3a-2127-422b-91ae-364da2661108
sgigate.sgi.com/security/20000803-01-A	af854a3a-2127-422b-91ae-364da2661108	sgigate.sgi.com/security/20000803-01-A
CVE Program record	CVE.ORG	www.cve.org/CVERecord?id=CVE-2020-10000
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2020-10000

No vendor comments have been submitted for this CVE.

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