



CVE-2004-0074

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2004-0074
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-02-17 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in xsok 1.02 allows local users to gain privileges via (1) a long LANG environment variable, or (2) a long PATH environment variable.

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Michael Bischoff	Xsok	1.02	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
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com
'xsok local games exploit' - MARC			af854a3a-2127-422b-91ae-364da2661108	marc.info
XSOK XSOKDir Option Local Buffer Overrun Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
XSOK LANG Environment Variable Local Buffer Overrun Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
'xsok local games exploit (2)' - MARC			af854a3a-2127-422b-91ae-364da2661108	marc.info
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.				