



Mapscrn 2.0.3 Stack-Based Buffer Overflow

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2017-20226
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-28 12:16:01 UTC
Updated	2026-05-01 14:41:28 UTC
Description	Mapscrn 2.0.3 contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitrary code by s

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000180000 probability, percentile 0.045330000 (date 2026-05-02)

Problem Types: CWE-787 | CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Msk	Mapscrm	affected 2.03	Not specified

References			
Reference	Source	Link	Tags
www.exploit-db.com/exploits/49144	disclosure@vulncheck.com	www.exploit-db.com	

www.exploit-db.com/exploits/42144	disclosure@vulncheck.com	www.exploit-db.com	
ccross.msk.su	disclosure@vulncheck.com	ccross.msk.su	
www.vulncheck.com/advisories/mapscrn-stack-based-buffer-overflow	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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