xwpe 1.5.30a-2.1 Stack-based Buffer Overflow

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

Summary

CVE	CVE-2016-20037
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-28 12:15:58 UTC
Updated	2026-05-01 15:21:32 UTC
Description	xwpe 1.5.30a-2.1 and prior contains a stack-based buffer overflow vulnerability that allows local attackers to execute arbitra

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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000180000 probability, percentile 0.045220000 (date 2026-05-05)

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/MSC: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	Identicalsoftware	XWPE	affected 1.5.30a-2.1	Not specified

References

Reference	Source	Link	Tags
www.vulncheck.com/advisories/xwpe-30a-stack-based-buffer-overflow	disclosure@vulncheck.com	www.vulncheck.com	

www.vulncheck.com/advisories/xwpe-30a-stack-based-buffer-overflow	disclosure@vulncheck.com	www.vulncheck.com	
www.identicalsoftware.com/xwpe	disclosure@vulncheck.com	www.identicalsoftware.com	
www.exploit-db.com/exploits/39285	disclosure@vulncheck.com	www.exploit-db.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

Vendor Comments And Credit

Discovery Credit

CNA: Juan Sacco - http://www.exploitpack.com < (en)

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