CVE-2014-8778

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

Summary

CVE	CVE-2014-8778
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-16 18:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Checkmarx CxSAST (formerly CxSuite) before 7.1.8 allows remote authenticated users to bypass the CxQL sandbox protec

Risk And Classification

Primary CVSS: v2.0 9 from nvd@nist.gov

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

Problem Types: CWE-94 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkmarx	Cxsast	All	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
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
Full Disclosure: Checkmarx CxQL Sandbox bypass (CVE-2014-8778)	af854a3a-2127-422b-91ae-364da2661108	seclists.org
Checkmarx CxQL 7.1.5 Sandbox Bypass ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packetstormsecurity.cor
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.