# CVE-2014-9765

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-9765 |
| **State** | PUBLISHED |
| **Assigner** | debian |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-04-19 21:59:01 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | Buffer overflow in the main_get_appheader function in xdelta3-main.h in xdelta3 before 3.0.9 allows remote attackers to ex |

## Risk And Classification

**Primary CVSS:** v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**Problem Types:** CWE-119 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.0 | nvd@nist.gov | Primary | 8.8 | HIGH | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 6.8 | | AV:N/AC:M/Au:N/C:P/I:P/A:P |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 15.10 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.1 | All | All | All |
| Operating System | Opensuse | Opensuse | 13.2 | All | All | All |
| Application | Xdelta | Xdelta3 | 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 |
|---|---|
| Add appheader tests; fix buffer overflow in main_get_appheader · jmacd/xdelta-gpl@ef93ff7 · GitHub | af854a3a-2127-422b-91ae-364da266 |
| oss-security - CVE request - buffer overflow in xdelta3 before 3.0.9 | af854a3a-2127-422b-91ae-364da266 |
| oss-security - Re: CVE request - buffer overflow in xdelta3 before 3.0.9 | af854a3a-2127-422b-91ae-364da266 |
| USN-2901-1: xdelta3 vulnerability \| Ubuntu | af854a3a-2127-422b-91ae-364da266 |

| | |
|---|---|
| Debian -- Security Information -- DSA-3484-1 xdelta3 | af854a3a-2127-422b-91ae-364da266 |
| openSUSE-SU-2016:0530-1: moderate: Security update for xdelta3 | af854a3a-2127-422b-91ae-364da266 |
| xdelta: User-assisted execution of arbitrary code (GLSA 201701-40) — Gentoo security | af854a3a-2127-422b-91ae-364da266 |
| xdelta3 CVE-2014-9765 Local Buffer Overflow Vulnerability | af854a3a-2127-422b-91ae-364da266 |
| openSUSE-SU-2016:0524-1: moderate: Security update for xdelta3 | af854a3a-2127-422b-91ae-364da266 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

671082 EulerOS Security Update for xdelta (EulerOS-SA-2019-2682)

710390 Gentoo Linux xdelta User-assisted execution of arbitrary code Vulnerability (GLSA 201701-40)