

## NATIONAL VULNERABILITY DATABASE



## VULNERABILITIES

## CVE-2014-9765 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Current Description

Buffer overflow in the main\_get\_appheader function in xdelta3-main.h in xdelta3 before 3.0.9 allows remote attackers to execute arbitrary code via a crafted input file.

[+View Analysis Description](#)

### Severity

CVSS Version 3.x

CVSS Version 2.0

#### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **8.8 HIGH**

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

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*


*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

## References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this

Hyperlink	Resource
<a href="http://lists.opensuse.org/opensuse-updates/2016-02/msg00125.html">http://lists.opensuse.org/opensuse-updates/2016-02/msg00125.html</a>	
<a href="http://lists.opensuse.org/opensuse-updates/2016-02/msg00131.html">http://lists.opensuse.org/opensuse-updates/2016-02/msg00131.html</a>	
<a href="http://www.debian.org/security/2016/dsa-3484">http://www.debian.org/security/2016/dsa-3484</a>	
<a href="http://www.openwall.com/lists/oss-security/2016/02/08/1">http://www.openwall.com/lists/oss-security/2016/02/08/1</a>	
<a href="http://www.openwall.com/lists/oss-security/2016/02/08/2">http://www.openwall.com/lists/oss-security/2016/02/08/2</a>	
<a href="http://www.securityfocus.com/bid/83109">http://www.securityfocus.com/bid/83109</a>	
<a href="http://www.ubuntu.com/usn/USN-2901-1">http://www.ubuntu.com/usn/USN-2901-1</a>	
<a href="https://github.com/jmacd/xdelta-devel/commit/ef93ff74203e030073b898c05e8b4860b5d09ef2">https://github.com/jmacd/xdelta-devel/commit/ef93ff74203e030073b898c05e8b4860b5d09ef2</a>	
<a href="https://security.gentoo.org/glsa/201701-40">https://security.gentoo.org/glsa/201701-40</a>	

## Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	 NIST

## Known Affected Software Configurations [Switch to CPE](#)

### 2.2


#### Configuration 1 ([hide](#))

 <b>cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*</b> <a href="#">Show Matching CPE(s)</a>
 <b>cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a>


#### Configuration 2 ([hide](#))

 <b>cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a>
 <b>cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a>

#### Configuration 3 ([hide](#))

 <b>cpe:2.3:a:xdelta:xdelta3:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a>	<b>Up to (including) 3.0.8</b>
---	--

#### Configuration 4 ([hide](#))

 <b>cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a>
 <b>cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*</b> <a href="#">Show Matching CPE(s)</a>

 Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

## Change History

6 change records found [show changes](#)

## QUICK INFO

### CVE Dictionary Entry:

[CVE-2014-9765](#)

### NVD Published Date:

04/19/2016

### NVD Last Modified:

10/30/2018

### Source:

Debian GNU/Linux



### HEADQUARTERS

100 Bureau Drive  
Gaithersburg, MD 20899  
(301) 975-2000

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

### Incident Response Assistance and Non-NVD Related

#### Technical Cyber Security Questions:

US-CERT Security Operations Center  
Email: [soc@us-cert.gov](mailto:soc@us-cert.gov)  
Phone: 1-888-282-0870

Sponsored by  
CISA



[Privacy Statement](#) | [Privacy Policy](#) | [Security Notice](#) | [Accessibility Statement](#) | [NIST Privacy Program](#) | [No Fear Act Policy](#) | [Disclaimer](#) |  
[FOIA](#) | [Environmental Policy Statement](#) | [Cookie Disclaimer](#) | [Scientific Integrity Summary](#) | [NIST Information Quality Standards](#) |  
[Commerce.gov](#) | [Healthcare.gov](#) | [Science.gov](#) | [USA.gov](#) |