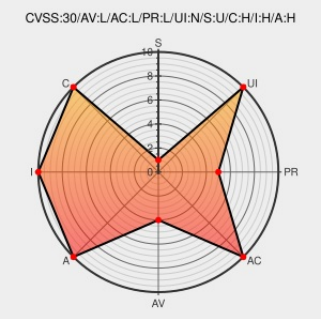
CVE-2014-9862

Published on: 07/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9862

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mac Os X from Apple contain the following vulnerability:

Integer signedness error in bspatch.c in bspatch in bsdiff, as used in Apple OS X before 10.11.6 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow) via a crafted patch file.

CVE-2014-9862 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
About the security content of OS X El Capitan v10.11.6 and Security Update 2016-004 - Apple Support	Vendor Advisory, support.apple.com, text/html	CONFIRM support.apple.com/HT206903
USN-4500-1: bsdiff vulnerabilities | Ubuntu	usn.ubuntu.com	UBUNTU USN-4500-1

security notices | Ubuntu	text/html	
oss-security - X41 D-Sec GmbH Security Advisory X41-2020-006: Memory Corruption Vulnerability in bspatch	www.openwall.com text/html	MLIST [oss-security] 20200709 X41 D-Sec GmbH Securi Vulnerability in bspatch
d0307d1711bd74e51b783a49f9160775aa22e659 - chromiumos/third_party/bsdiff - Git at Google	Issue Tracking chromium.googlesource.com text/html	CONFIRM chromium.googlesource.com/chromiumos/third_party/bsdiff/
[SECURITY] [DLA 2010-1] bsdiff security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20191126 [SECURITY] [DL
Apple Mac OS X APPLE-SA-2016-07-18-1 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 91824
APPLE-SA-2016-07-18-1 OS X El Capitan v10.11.6 and Security Update 2016-004	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-07-18-1
372525 - chromium - An open-source project to help move the web forward. - Monorail	Issue Tracking bugs.chromium.org text/html	CONFIRM bugs.chromium.org/p/chromium/issues/detail?
Binary diff: Heap-based buffer overflow (GLSA 202003-44) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202003-44
	security.FreeBSD.org text/plain	FREEBSD FreeBSD-SA-16:25
4d054795b673855e3a7556c6f2f7ab99ca509998 - platform/external/bsdiff - Git at Google	Issue Tracking android.googlesource.com text/html	CONFIRM android.googlesource.com/platform/external/bsdiff/+/4d0547
openSUSE-SU-2016:1977-1: moderate: Security update for bsdiff	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1977
Full Disclosure: X41 D-Sec GmbH Security Advisory X41-2020-006: Memory Corruption Vulnerability in bspatch	seclists.org text/html	FULLDISC 20200709 X41 D-Sec GmbH Security Adviso in bspatch
FreeBSD bsdiff Heap Overflow in Processing Patch Files Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036438

Related QID Numbers

752550 SUSE Enterprise Linux Security Update for libostree (SUSE-SU-2022:3094-1)

752634 SUSE Enterprise Linux Security Update for libostree (SUSE-SU-2022:3456-1)

752636 SUSE Enterprise Linux Security Update for libostree (SUSE-SU-2022:3455-1)

752690 SUSE Enterprise Linux Security Update for libostree (SUSE-SU-2022:3671-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→