



CVE-2020-14315

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-14315
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-16 14:15:00 UTC
Updated	2022-01-01 18:38:00 UTC
Description	A memory corruption vulnerability is present in bspatch as shipped in Colin Percival's bsdiff tools version 4.3. Insufficient ch

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Daemonology	Bsdiff	4.3	All	All	All
Application	Daemonology	Bsdiff	4.3	All	All	All

References

Reference	Source	Link
Advisory X41-2020-006: Memory Corruption Vulnerability in bspatch X41 D-SEC GmbH	MISC	www.x41dsec.com
oss-security - X41 D-Sec GmbH Security Advisory X41-2020-006: Memory Corruption Vulnerability in bspatch	MISC	www.oss-security.com
1856747 – (CVE-2020-14315) CVE-2020-14315 bsdiff: handling external inputs allows attacker to bypass sanity checks	MISC	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180796 Debian Security Update for bsdiff (CVE-2020-14315)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)