



CVE-2019-9075

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

Summary

CVE	CVE-2019-9075
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-24 00:29:00 UTC
Updated	2021-12-10 20:19:00 UTC
Description	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is a h

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	F5	Big-ip Access Policy Manager	14.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	15.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	14.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	15.0.0	All	All	All
Application	F5	Big-ip Analytics	14.1.0	All	All	All
Application	F5	Big-ip Analytics	15.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	14.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	15.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	14.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	15.0.0	All	All	All
Application	F5	Big-ip Domain Name System	14.1.0	All	All	All
Application	F5	Big-ip Domain Name System	15.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	14.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	15.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	14.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	15.0.0	All	All	All

Application	F5	Big-ip Global Traffic Manager	14.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	15.0.0	All	All	All
Application	F5	Big-ip Link Controller	14.1.0	All	All	All
Application	F5	Big-ip Link Controller	15.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	14.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	15.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	14.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	15.0.0	All	All	All
Application	F5	Big-ip Policy Webaccelerator	14.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	15.0.0	All	All	All
Application	Gnu	Binutils	2.32	All	All	All
Application	Gnu	Binutils	2.32	All	All	All
Application	Netapp	Element Software Management	All	All	All	All
Application	Netapp	Element Software Management	All	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1804-1: moderate: Security update f	SUSE	lists.opensuse.org	
Binutils: Multiple vulnerabilities (GLSA 202107-24) — Gentoo security	GENTOO	security.gentoo.org	
USN-4336-1: GNU binutils vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
February 2019 GNU Binutils Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Patch, Third I
24236 – size: Heap buffer overflow in _bfd_archive_64_bit_slurp_armap	MISC	sourceware.org	Exploit, Issue
support.f5.com/csp/article/K42059040	CONFIRM	support.f5.com	
[security-announce] openSUSE-SU-2020:1790-1: moderate: Security update f	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296077](#) Oracle Solaris 11.4 Support Repository Update (SRU) 18.4.0 Missing (CPUJAN2020)

[377579](#) Alibaba Cloud Linux Security Update for binutils (ALINUX3-SA-2022:0120)

[710052](#) Gentoo Linux Binutils Multiple vulnerabilities (GLSA 202107-24)

751313 SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2021:3593-1)

900079 CBL-Mariner Linux Security Update for binutils 2.32

902860 Common Base Linux Mariner (CBL-Mariner) Security Update for binutils (1900)

© [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](#).

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