



CVE-2016-9801

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

Summary

CVE	CVE-2016-9801
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-03 06:59:00 UTC
Updated	2016-12-07 19:32:00 UTC
Description	In BlueZ 5.42, a buffer overflow was observed in "set_ext_ctrl" function in "tools/parser/l2cap.c" source file when processing

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bluez	Bluez	5.42	All	All	All
Application	Bluez	Bluez	5.42	All	All	All

References

Reference	Source	Link	Tags
multiple buffer overflows and out-of-bound reads — Linux Bluetooth	MISC	www.spinics.net	Exploit, Third Party Advisory
BlueZ Buffer Overflow and Denial of Service Vulnerabilities	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)