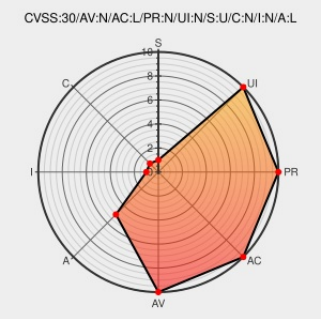
# CVE-2016-9798

Published on: 12/03/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:17 PM UTC

## CVE-2016-9798

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




Certain versions of Bluez from Bluez contain the following vulnerability:

In BlueZ 5.42, a use-after-free was identified in "conf_opt" function in "tools/parser/l2cap.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.

CVE-2016-9798 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.3 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | LOW |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| multiple buffer overflows and out-of-bound reads — Linux Bluetooth | Exploit, Third Party Advisory, www.spinics.net, text/html | MISC www.spinics.net/lists/linux-bluetooth/msg68892.html |

| | | |
|---|---|---|
| [security-announce] openSUSE-SU-2019:1476-1: moderate: Security update f | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2019:1476 |
| [security-announce] openSUSE-SU-2019:2585-1: moderate: Security update f | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2019:2585 |
| [security-announce] openSUSE-SU-2019:2588-1: moderate: Security update f | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2019:2588 |
| BlueZ Buffer Overflow and Denial of Service Vulnerabilities | Third Party Advisory<br>VDB Entry<br>cve.report (archive)<br>text/html | BID 94652 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:bluez:bluez:5.42:*:*:*:*:*:*:*:

cpe:2.3:a:bluez:bluez:5.42:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→