



CVE-2017-1000251

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

Summary

CVE	CVE-2017-1000251
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-12 17:29:00 UTC
Updated	2023-01-19 15:53:00 UTC
Description	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

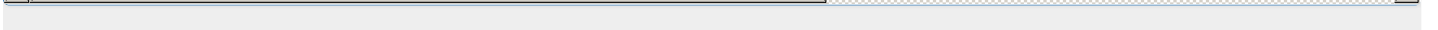
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Nvidia	Jetson Tk1	r21	All	All	All
Application	Nvidia	Jetson Tk1	r24	All	All	All
Application	Nvidia	Jetson Tk1	r21	All	All	All
Application	Nvidia	Jetson Tk1	r24	All	All	All
Application	Nvidia	Jetson Tx1	r21	All	All	All
Application	Nvidia	Jetson Tx1	r24	All	All	All
Application	Nvidia	Jetson Tx1	r21	All	All	All
Application	Nvidia	Jetson Tx1	r24	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source
Linux Kernel < 4.13.1 - BlueTooth Buffer Overflow (PoC)	EXP
Red Hat Customer Portal	RED
Vulnerability Note VU#240311 - Multiple Bluetooth implementation vulnerabilities affect many devices	CER
Security Bulletin: NVIDIA Tegra Jetson L4T contains multiple vulnerabilities; updates for "BlueBorne" and "Dnsmasq". NVIDIA	CON
Blueborne - Linux Kernel Remote Denial of Service in Bluetooth subsystem - CVE-2017-1000251 - Red Hat Customer Portal	CON
Red Hat Customer Portal	RED
BlueBorne Information from the Research Team - Armis Labs	MISC
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
Bluetooth: Add configuration support for ERTM and Streaming mode · torvalds/linux@f2fcfd · GitHub	MISC
Linux Kernel Bluetooth Subsystem CVE-2017-1000251 Stack Based Buffer Overflow Vulnerability	BID

Red Hat Customer Portal	RED
Synology-SA-17:52 BlueBorne Synology Inc.	CON
Linux Kernel Stack Overflow in Bluetooth Stack Lets Remote Users on the Wireless Network Execute Arbitrary Code - SecurityTracker	SEC
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
Debian -- Security Information -- DSA-3981-1 linux	DEB
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
CVE Program record	CVE
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

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

© [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](#)