CVE-2015-8612

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-8612
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-08 19:59:00 UTC
Updated	2019-01-17 11:29:00 UTC
Description	The EnableNetwork method in the Network class in plugins/mechanism/Network.py in Blueman before 2.0.3 allows local us

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Blueman Project	Blueman	All	All	All	All

References

Reference
Privilege escalation in blueman dbus API · Issue #416 · blueman-project/blueman · GitHub
the grugq on Twitter: "7350greenman [~]> D=org.blueman.Mechanism;gdbus call -y -d $D -o / -m ${D}.EnableNetwork '[]' '[]' "os.chmod('/bin/s
Debian -- Security Information -- DSA-3427-1 blueman
blueman - set_dhcp_handler D-Bus Privilege Escalation (Metasploit) - Linux local Exploit
Release 2.0.3 · blueman-project/blueman · GitHub
Slackware Security Advisory - blueman Updates ≈ Packet Storm
oss-security - CVE request: Blueman: Privilege escalation in blueman dbus API
oss-security - Re: CVE request: Blueman: Privilege escalation in blueman dbus API
Blueman CVE-2015-8612 Remote Privilege Escalation Vulnerability
The Slackware Linux Project: Slackware Security Advisories
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**