Security Advisory Report - OBSO-1710-01

Linux Kernel bluetooth Remote Stack Buffer Overflow (BlueBorne) (CVE-2017-1000251)

Creation Date: 2017-10-06
Last Update: 2017-11-03

Summary

Armis Labs researchers have discovered eight vulnerabilities codenamed collectively as BlueBorne in the Bluetooth implementations used by over 5.3 billion devices.

No user interaction is needed for an attacker to use the BleuBorne flaws, nor does the attacker need to pair with a target device.
BlueBorne affects all Bluetooth enabled devices that use the BlueZ protocol stack.

They affect the Bluetooth implementations in Android, iOS, Microsoft, and Linux, impacting almost all Bluetooth device types, from smartphones to laptops, and from IoT devices to smart cars.
Three of these eight security flaws are rated critical and according to researchers at Armis the IoT security company that discovered BlueBorne they allow attackers to take over devices and execute malicious code, or to run Man-in-the-Middle attacks and intercept Bluetooth communications.

Armis warns of attacks that combine physical presence with the BlueBorne flaws.
For example, a delivery person dropping a package at a bank could carry weaponized code on a BlueTooth-enabled device.
Once he enters the bank, his device infects others and grants attackers a foothold on a previously secured network.

All Android phones, tablets, and wearables of all versions are affected by the four above mentioned vulnerabilities.
Android devices using Bluetooth Low Energy only are not affected.
Google patched the flaws in its September Android Security Bulletin.

Windows versions since Windows Vista are all affected. Microsoft said Windows phones are not impacted by BlueBorne.
Microsoft secretly released patches in July for CVE-2017-8628, but only recently included details about the fixed vulnerability in September's Patch Tuesday.

All Linux devices running BlueZ are affected by an information leak, while all Linux devices from version 3.3-rc1 (released in October 2011) are affected by a remote code execution flaw that can be exploited via Bluetooth. Samsung's Tizen OS, based on Linux, is also affected.

All iPhone, iPad and iPod touch devices with iOS 9.3.5 and lower, and AppleTV devices with version 7.2.2 and lower are affected, but the issue was patched in iOS 10.

Disable Bluetooth unless you need to use it, but then turn it off immediately.
When a patch or update is issued and installed on your device, you should be able to turn Bluetooth back on and leave it on safely.

Users of Android devices can determine if their device is vulnerable by downloading the BlueBorne Android App on the Google Play Store and use it to run a simple and quick check

https://www.bleepingcomputer.com/news/security/blueborne-vulnerabilities-impact-over-5-billion-bluetooth-enabled-devices/

Vulnerability Details

Linux Kernel contains an overflow condition in the l2cap_parse_conf_rsp() function in net/bluetooth/l2cap_core.c that is triggered when parsing L2CAP EFS configuration responses.
With specially crafted Bluetooth packets, a proximate attacker can cause a stack-based buffer overflow and potentially execute arbitrary code.

The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3-rc1 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.

This vulnerability is an RCE vulnerability in the Kernel's implementation of Bluetooth's L2CAP (net/bluetooth/l2cap_core.c):
...
The function l2cap_parse_conf_rsp parses the configuration elements in the configuration response (rsp->data), and copies them (after validating them) to the output buffer (buf).

The function does not receive a maximum length of the output buffer, and this buffer is allocated on the stack of l2cap_config_rsp.
So sending a configuration response which contains a large number of configuration elements (they can also be the same type of element repeated multiple times) - would cause a stack overflow of the output buffer (buf).

Reaching this case (L2CAP_CONF_PENDING) is achievable by sending a configuration request with an EFS element, and setting the stype field to L2CAP_SERV_NOTRAFIC, prior to the crafted configuration
response that would trigger the stack overflow.

A patch for this vulnerability was pushed to upstream Linux Kernel:

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=e860d2c904d1a9f38a24eb44c9f34b8f915a6ea3

http://seclists.org/oss-sec/2017/q3/439

Exploit/ PoC:

https://www.exploit-db.com/exploits/42762/

Related vulnerabilities

- Information Leak Vulnerability in Android (CVE-2017-0785)
- Remote Code Execution Vulnerability (CVE-2017-0781) in Android's Bluetooth Network Encapsulation Protocol (BNEP) service
- Remote Code Execution Vulnerability (CVE-2017-0782) in Android BNEP's Personal Area Networking (PAN) profile
- The Bluetooth Pineapple in Android&mdash;Logical flaw (CVE-2017-0783)
- Linux kernel Remote Code Execution vulnerability (CVE-2017-1000251)
- Linux Bluetooth stack (BlueZ) information leak vulnerability (CVE-2017-1000250)
- The Bluetooth Pineapple in Windows&mdash;Logical flaw (CVE-2017-8628)
- Apple Low Energy Audio Protocol Remote Code Execution vulnerability (CVE-2017-14315)

Affected Products

On the OpenScape Desk Phone CP 600 phone, Bluetooth is available and allows use of Bluetooth headsets, transfer of contact information (vcard), proximity monitoring and Eddystone beacon and iBeacon.
The stack used is BSA, not BlueZ, so the CP 600 phone is not affected.

On OpenStage 60 and OpenStage 80 phones Bluetooth is available and allows use of Bluetooth headsets or transfer of contact information (vcard).
Investigations with the PoC and OpenStage 60/80 phones did not crash the phone.
So the vulnerability is rated medium at the most.

For OpenStage 60 and 80 SIP a fix is in version V3 R5.8.0

For OpenStage 60 and 80 HFA a fix is in version V3 R0.40.0

Both versions are planned to be GA on Nov 3rd.

All other phone types do not support Bluetooth so they are not vulnerable.

All other Unify products do not support Bluetooth.

Recommended Actions

The Security Checklist for OpenStage 60/80 already recommends:
If Bluetooth is enabled then the method of pairing can be set to be automatic or needing a prompt. To ensure that the user is aware when another device is paired with their phone and to prevent unauthorised pairing the pairing method should be set to prompt and the pairing PIN must be set by the user.
If Bluetooth is enabled then to reduce possibility of unauthorised pairing attempts the discoverable parameter should only be set to YES by the user when needed for pairing.

As the main use for Bluetooth on OpenStage 60/80 phones is for headsets, Unify already recommend Bluetooth is disabled for those customers that do not use Bluetooth headsets.

Apply the fix versions:

For OpenStage 60 and 80 SIP a fix is in version V3 R5.8.0

For OpenStage 60 and 80 HFA a fix is in version V3 R0.40.0

For those customers that use Bluetooth headsets, there is a medium risk of possible infection and this risk can be reduced further by switching off discoverability by other Bluetooth enabled devices.

References

http://seclists.org/oss-sec/2017/q3/439

https://www.bleepingcomputer.com/news/security/blueborne-vulnerabilities-impact-over-5-billion-bluetooth-enabled-devices/

https://threatpost.com/wireless-blueborne-attacks-target-billions-of-bluetooth-devices/127921/

http://thehackernews.com/2017/09/blueborne-bluetooth-hacking.html

http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf

https://www.youtube.com/watch?v=U7mWeKhd_-A

https://www.exploit-db.com/exploits/42762/

https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00043.html

https://play.google.com/store/apps/details?id=com.armis.blueborne_detector

Revision History

First Draft 2017-09-27

First release 2017-10-06

Update 2017-11-03

Advisory ID: OBSO-1710-01 (a=167), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.
All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.