(Mobile Pwn2Own) Google Android Bluetooth Forced Pairing Vulnerability

http://www.zerodayinitiative.com/advisories/ZDI-15-092/

ZDI-15-092: March 12th, 2015

CVE ID

CVE-2014-7914

CVSS Score

4.8, (AV:A/AC:L/Au:N/C:P/I:P/A:N)

Affected Vendors

Google

Affected Products

Android

Vulnerability Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Google Android. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the Bluetooth application stack allowing for arbitrary Host Controller Interface commands to be issued without prior pairing. By obtaining a Bluetooth address, creating and emulating a Bluetooth out-of-band 'handover' NFC NDEF tag, and sniffing encryption keys and exchanging them with the device, an attacker can force pairing with a Bluetooth device. A remote attacker can use this to achieve remote code execution under the context of the process.

Vendor Response

Google has issued an update to correct this vulnerability. More details can be found at:

https://android.googlesource.com/platform/external/bluetooth/bluedroid/+/0360aa7c418152a3e5e335a065ac3629cbb09559

Disclosure Timeline

2014-11-19 - Vulnerability reported to vendor
2015-03-12 - Coordinated public release of advisory

Credit

This vulnerability was discovered by: **Adam Laurie Aperture Labs**

info@aperturelabs.com

www.aperturelabs.com