Security Advisory 2017-09-25-01 - “BlueBorne” Linux Vulnerabilities

Summary

A series of vulnerabilities associated with particular implementations of the Bluetooth Specification, referred to as “BlueBorne”, were discovered and released in September 2017. These vulnerabilities, if exploited, could provide the attacker with control over the affected devices.

The specific vulnerabilities are the following:

1. Linux kernel RCE vulnerability - CVE-2017-1000251
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000251
2. Linux Bluetooth stack (BlueZ) information Leak vulnerability - CVE-2017-1000250
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000250

Affected Products

Pwn Pro
Pwn Pro Plus
Pwn Plug R3
Pwn Plug R4

Workaround

The only known workaround is to disable Bluetooth completely on the devices. Please contact support@pwnieexpress.com for instructions on how to perform this action.

Software Patches

There are currently no patches available for these vulnerabilities. We will create an update pack as soon as a patch to the vulnerabilities is available.