Common Vulnerabilities and Exposures

Version 1.0 *February 2016*

This document lists common vulnerabilities and exposures (CVE) for Laird's Connectivity Solutions products.

Below is a list and explanation of announced CVEs related to Laird products.

- CVE-2016-0777 and CVE-2016-0778
- CVE-2016-0728

OpenSSH Roaming Vulnerabilities

Announced 14 January 2016

CVE-2016-0777 and CVE-2016-0778

Qualys announced two vulnerabilities in OpenSSH clients from version 5.4 to 7.1 (inclusive). These vulnerabilities are associated with the experimental support for SSH connection roaming in the SSH client. One vulnerability is a buffer overflow issue and the other is an exploit for leaking information including private keys.

These vulnerabilities do affect current versions of the software across our Linux WB line, however they are considered to be of minimal concern to our customers. Most SSH use on the WB is as a server; SSHD is not affected by this issue.

These vulnerabilities can only be triggered by using the SSH client on the WB to connect to a malicious or compromised server. Use of the SSH client on the WB by customers is unusual and not a normally-expected use case. Hence we do not consider this a significant problem for users of the WB.

These exploits have been fixed in OpenSSH 7.1p1; this fix will be put into our next GA5 release of the WB software. Our next GA4 point release will have the vulnerable features turned off.

If concerned, customers using GA3 or earlier that are not upgrading may turn off the feature by adding 'UseRoaming no' to the global ssh_config(5) file /etc/ssh/ssh_config or by passing -oUseRoaming=no on the command line when using the SSH client.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

LINUX KEYRING VULNERABILITY

Announced 14 January 2015

CVE-2016-0728

Announced by a commercial security consulting company, CVE-2016-0728 references a potential security issue in the Linux kernel past version 3.8. This issue refers to the keyctl API provided by the Linux kernel to provide user-space keyring management.

Laird's Linux-based Wi-Fi products like the WB series are not directly vulnerable to this issue. While the API exists in our kernel, no current code utilizes this API. The vulnerability cannot be triggered by remote methods, so an attacker would already have to have physical access to be able to place code on the device to access the possible vulnerability.

Even if triggered, the vulnerability would not allow an attacker to gain any advantage over the system they could not have already had. The primary risk posed by exploiting this bug is privilege escalation. The WB is not designed as a server or a multi-user system and as such there is no risk of privilege escalation.

While the possible vulnerability cannot be remotely triggered, code can be written and placed on a WB that could trigger the vulnerability. Customers are advised not to run arbitrary code that they have not created or vetted themselves or has not been provided by Laird as part of the WB package. Of course, as already stated, exploitation of this vulnerability on a WB is largely academic and even if exploited it would be unlikely to cause any additional issues.

As a fix for the issue is developed, we will include it in future releases of the WB software. As we view the risk of CVE-2016-0728 to be low in the case of the WB, at this time we do not intend to back-port the fix to older releases.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610