153 Somerford Road, Christchurch, Dorset, BH23 3TY, UK
Tel: +44 (0)1425 270333 Fax: +44 (0)1425 270433
Web: www.datatrackplc.com Email: admin@dtrack.com

# Linux "Ghost" Remote Code Execution Vulnerability

## Security Advisory – 02 Feb 2015

The following is an extract of **Debian Security Advisory DSA-2142-1** dated 27th January 2015 which relates to security vulnerabilities in the **eglibc** package. The issue affects Tracker 2800 devices running OS version 40106 or earlier. The fixed version has been incorporated in Tracker 2800 OS version 40107 which is currently being tested and due for release by 10 February 2015. We recommend that Tracker 2800 units are upgraded as soon as possible. No other Data Track products are affected.

*Debian Security Advisory*

*DSA-3142-1 eglibc -- security update*

*Reported 27 Jan 2015*

*Several vulnerabilities have been fixed in eglibc, Debian's version of the GNU C library:*

*CVE-2015-0235*

*Qualys discovered that the gethostbyname and gethostbyname2 functions were subject to a buffer overflow if provided with a crafted IP address argument. This could be used by an attacker to execute arbitrary code in processes which called the affected functions.*

*The original glibc bug was reported by Peter Klotz.*

*CVE-2014-7817*

*Tim Waugh of Red Hat discovered that the WRDE_NOCMD option of the wordexp function did not suppress command execution in all cases. This allows a context-dependent attacker to execute shell commands.*

*CVE-2012-6656 CVE-2014-6040*

*The charset conversion code for certain IBM multi-byte code pages could perform an out-of-bounds array access, causing the process to crash. In some scenarios, this allows a remote attacker to cause a persistent denial of service.*

*For the stable distribution (wheezy), these problems have been fixed in version 2.13-38+deb7u7.*

The original Debian document is available at https://www.debian.org/security/2015/dsa-3142

Please contact Data Track Technology plc if further information and support is required.