GNU Bash "Shellshock" Security Vulnerability

December 5, 2014

A critical security vulnerability has been reported in the GNU Bash "Shellshock", which is a common command line used in many Linux/UNIX operating systems.

TA Triumph-Adler GmbH has investigated whether or not its products, software and services are affected. The results are as follows.

Printers/MFPs

TA Triumph-Adler and UTAX products use a special embedded version of the Linux Operating System. There is no access to the Bash prompt from the network, operation panel, USB, or any other interface, therefore, TA Triumph-Adler and UTAX printers and MFPs are not susceptible to the “Shellshock” vulnerability.

Connectivity Options

"Bash" environment is not implemented in following TA Triumph-Adler and UTAX optional products, and therefore unaffected.

FAX System (*)

IB-23/IB-50/IB-51 / IB-110

Software, Utilities

"Bash" environment is not implemented in any TA Triumph-Adler and UTAX software/utilities and therefore unaffected.

EFI™ Fiery Printing System(s)

The Fiery Printing System, optional on select KYOCERA color MFPs, uses an embedded Linux Operating System. EFI, the manufacturer of Fiery Printing Systems, has identified a vulnerability that they regard as a low security risk. EFI has created a patch to address the Shellshock vulnerability (Patch FIT 100698425.ps) that was made available on December 1st 2014. More information, as well as the patch itself, for all Linux based Fiery printer servers is available through EFIs System Update and Web Update. It is strongly recommended by EFI that this patch be immediately implemented to all potentially affected Fiery Printing Systems. For more information please speak with your local authorized dealer/reseller.

TA Cockpit / UTAX Smart

TA Cockpit and UTAX Smart use an embedded Linux Operating System. TA Triumph-Adler GmbH, the manufacturer of TA Cockpit / UTAX Smart, has identified a vulnerability that they regard as a low security risk. TA Triumph-Adler GmbH is currently working on a firmware patch, which will resolve this vulnerability, and it will be made available before January 1, 2015.