

Epson Professional Imaging Support Notice of Firmware Vulnerability

Epson is announcing important firmware updates for the Webconfig feature in certain Professional Imaging Printer products. This update addresses a vulnerability that may compromise the security of the printer's web browser. The CVE-ID for this vulnerability is CVE-2017-6443 and you can learn more about it on the CVE website, at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6443>.

The list below reflects the affected SKUs. The updated firmware and instructions for download can be found at <https://epson.com/support/security>. End-users are urged to update their firmware immediately.

Products for which Firmware Updates are Now Available		Affected Firmware Versions
Epson Stylus Pro WT7900	All Models	All Versions
Epson SureColor F2000	All Models	All Versions
Epson Stylus Pro 4900	All Models	All Versions
Epson Stylus Pro 7900	All Models	All Versions
Epson Stylus Pro 9900	All Models	All Versions
Epson Stylus Pro 7890	All Models	All Versions
Epson Stylus Pro 9890	All Models	All Versions
Epson Stylus Pro 4880	All Models	All Versions
Epson Stylus Pro 4450	All Models	All Versions
Epson Stylus Pro 11880	All Models	All Versions
Epson Stylus Pro GS6000	All Models	All Versions
Epson Stylus Pro 3800	All Models	All Versions
Epson Stylus Pro 3880	All Models	All Versions

In addition, as a general rule to help secure all devices, end-users and their administrators should always implement and maintain industry-standard security controls and practices in setting up and managing their networks. Those practices include immediately replacing default passwords with strong passwords and installing printer software behind a firewall.

Additionally, Epson always recommends that end users routinely check for firmware updates and keep their Professional Imaging Products updated to the latest firmware to achieve the best possible performance from their products.

If you have questions about this notice, you may contact Epson at 1-800-377-6611/ 562-276-1305, or contact your Epson Professional Imaging Account Manager. End-users can access ongoing updates regarding the availability of firmware updates and instructions at: <https://epson.com/support/security>.