

(English)

27 July 2026

Dear All,

Regarding Network Scanner Tool Lite/Network Scanner Tool Security Vulnerability and Countermeasures

Thank you for your continuous support.

We have been reported a vulnerability summarized as below in Network Scanner Tool Lite. We have released software updates against the vulnerability. We apologize for the inconvenience, however, please inform your customers, dealers, and other relevant parties of "Application of the security countermeasures" described as the bottom in this letter. Also please prompt them to apply the updated software.

■ Abstract of the vulnerability

Abstract of the vulnerability that we disclose this time are as follows:

- Malicious attackers may gain unauthorized access to a PC on which the product is installed and running, or send malicious files to it and open/execute the files, potentially enabling attacks on other devices via that PC.

■ Conditions to enable attacks using the vulnerability

To enable attackers to successfully attack the MFP from outside of the corporate network using the vulnerability, the following conditions shall be fulfilled:

- The attacker is able to access the corporate network to which the MFP is connected
- The attacker knows the information that users cannot know through normal operation

The other cases, e.g., access to the MFP is properly protected have no impacts from attacks via the network regarding this vulnerability.

■ Affected software versions and status of preparation of the countermeasure

The following software versions are impacted by the vulnerability. They need software update to mitigate it. The updated software for Network Scanner Tool Lite is provided via the SHARP Software download website (see PRCG-26-7192, issued on 22 July 2026).

Product name	Software version affected (see note)	Note
Network Scanner Tool Lite V2.0.13	V2.0.13.3 and earlier	

The following versions are also impacted by the vulnerabilities, however, since the software support for these versions has ended, please prompt your customers to implement the above mitigation measures or consider discontinuing use of the software or upgrading to a successor version:

Product name	Software version
Network Scanner Tool Lite	All versions earlier than or equal to V2.0.11.14

■ Application of security countermeasures

Regardless of applying the firmware updates above, please make sure your customers' devices have been applied the following countermeasures in their site to reduce the possibility of attacks exploiting these vulnerabilities.

- Do not connect MFPs directly to the Internet. Connect them via a firewall or similar network appliance.
- Change admin password from factory default and manage it appropriately.
- Restrict device web page access via password (enable [System Settings]-[Security Settings]-[Password Change]-[Restrict Device Web Page Access Via Password]).

Not applying these countermeasures will increase possibilities for allowing malicious 3rd parties to attack the MFPs to get damages such as disabling the MFPs to boot, leaking data in the MFPs, etc.