

[Home](#)[Products](#)[Solutions](#)[Services](#)[Download & Videos](#)[Corporate Data](#)

## Response to vulnerability in some Toshiba Tec's digital multi-function peripherals

June 25, 2025  
Toshiba Tec Corporation

Thank you for using our products.

The following vulnerabilities have been identified in some of our multi-function peripherals. This issue does not result in the leakage of information from the product to outside parties.

### Vulnerability details

Target Products : e-STUDIO 301DN/ 302DNF (These products have been sold only in the Chinese market.)

For more information, see the reference sites below (Jump to another website with opening new window.):

Reference	Reference site
CVE-2017-9765 JVNVU#98807587	<a href="https://www.cve.org/CVERecord?id=CVE-2017-9765">https://www.cve.org/CVERecord?id=CVE-2017-9765</a> Stack Buffer Overflow Vulnerability
CVE-2024-2169 VNVU#93188600	<a href="https://www.cve.org/CVERecord?id=CVE-2024-2169">https://www.cve.org/CVERecord?id=CVE-2024-2169</a> Infinite loop of messages between servers
CVE-2024-51977 JVNVU#90043828	<a href="https://www.cve.org/CVERecord?id=CVE-2024-51977">https://www.cve.org/CVERecord?id=CVE-2024-51977</a> Possibility of information leakage in the printer
CVE-2024-51978 JVNVU#90043828	<a href="https://www.cve.org/CVERecord?id=CVE-2024-51978">https://www.cve.org/CVERecord?id=CVE-2024-51978</a> Possibility of authentication bypass
CVE-2024-51980 JVNVU#90043828	<a href="https://www.cve.org/CVERecord?id=CVE-2024-51980">https://www.cve.org/CVERecord?id=CVE-2024-51980</a> Possibility of being forced to connect to TCP
CVE-2024-51981 JVNVU#90043828	<a href="https://www.cve.org/CVERecord?id=CVE-2024-51981">https://www.cve.org/CVERecord?id=CVE-2024-51981</a> Possibility of arbitrary HTTP request execution
CVE-2024-51983 JVNVU#90043828	<a href="https://www.cve.org/CVERecord?id=CVE-2024-51983">https://www.cve.org/CVERecord?id=CVE-2024-51983</a> External attacks can cause your device to crash
CVE-2024-51984 JVNVU#90043828	<a href="https://www.cve.org/CVERecord?id=CVE-2024-51984">https://www.cve.org/CVERecord?id=CVE-2024-51984</a> Possibility of information leakage in the printer due to passback attacks

### Solution

Ask your service company to update the main unit software.

### Workaround

If you are using a product for which the firmware is not yet available, please use the workaround methods below.

1. Make sure you use the printer in a firewall-protected network environment in the office or with a router at home.
2. In addition, if necessary, change the following settings individually from "Web browser settings" of the product itself.

Reference	Workaround
CVE-2017-9765	Disable the WSD function.

CVE-2024-2169	Disable TFTP.
CVE-2024-51977	Disable "Web browser settings" on the product itself.
CVE-2024-51978	Change the administrator password from the default value.
CVE-2024-51980	Disable the WSD function.
CVE-2024-51981	Disable the WSD function.
CVE-2024-51983	Disable the WSD function.
CVE-2024-51984	Change the administrator password from the default value.

### Acknowledgements

We would like to thank Yepeng Pan of CISP, Germany, for reporting this vulnerability (CVE-2024-2169).

We would like to thank Stephen Fewer, Principal Security Researcher at Rapid7, USA, for reporting these vulnerabilities (CVE-2024-51977 - CVE-2024-51984).

[> Information Archives](#)

Toshiba Tec Group Philosophy  
**Creating with You**

