Command execution vulnerability in Epson WebConfig

Vulnerability Reference: CVE-2025-66635

Description:

An administrator password is required to log in to WebConfig.

A malicious third party who obtains the administrator password can execute arbitrary commands by logging in to Web Config and entering a specific string on a specific screen.

Impact:

The product settings could be reset or ping packets could be sent to other devices.

There are no reports of attacks exploiting this vulnerability until now.

Solution:

We strongly recommend applying a fixed firmware or taking workaround to mitigate the impact of this vulnerability

- ➢ Apply fixed firmware:

  For products that are currently on sale, we have released fixed firmware as listed below. Please download it from the Epson website and apply the update.
- ➢ Take workaround:

  To ensure the security of your Epson product, we recommend end-users and their administrators to implement and maintain industry-standard security controls and practices in setting up and managing password and network to which the product is connected.

  <Administrator Password >

  - ✓ Please set a unique password for each product.
  - ✓ The administrator password should be a complex string of characters that is difficult for others to guess, such as eight or more characters that contain not only English letters but also symbols and numbers.

  <Internet Connection>

  - ✓ Do not connect the product directly to the Internet; install it within a network protected by a firewall.
  - ✓ Please set a private IP address for the product.

  For more information on securing your Epson product, please refer “Security Guidelines”.

  The security guidelines are available on the following website:

  Security for printers and MFPs

Affected Products

➢ Large Format Printers

SC-T3255, SC-T3250, SC-T3200, SC-T3280, SC-T3270, SC-T5255, SC-T5250, SC-T5200, SC-T5280, SC-T5270, SC-T7255, SC-T7280, SC-T7270, SC-T7250, SC-T7200, SC-T5255D, SC-T5250D, SC-T5200D, SC-T5280D, SC-T5270D, SC-T7255D, SC-T7250D, SC-T7200D, SC-T7280D, SC-T7270D, SC-P10070, SC-P10080, SC-P10000, SC-P10050, SC-P20070, SC-P20000, SC-P20080, SC-P20050, SC-P7070, SC-P7050, SC-P7080, SC-P7000, SC-P9070, SC-P9050, SC-P9080, SC-P9000, SC-P6000, SC-P6050, SC-P6070, SC-P6080, SC-P8070, SC-P8050, SC-P8080, SC-P8000, SC-P10080D

➢ POS Printers

M-P60II, TM-P80, TM-P20, TM-m10, TM-m30, TM-T20II(**7), TM-T20II-m, TM-T88VI, TM-T88VI-iHUB, TM-H6000V, TM-T100E, TM-T100M, TM-T100N, TM-T100S, TM-T100W, TM-T20IIIL, TM-T20X, TM-T81III, TM-T82IIIL, TM-T82X, TM-T83III, TS-100, TM-T20III, TM-T82III, TM-m30II, TM-m30II-H, TM-m50, TM-m30II-NT, TM-m30II-S, TM-m30II-SL, TM-L100, UB-R04, UB-E04, UB-R05