Vulnerability in EPSON WebConfig / Epson Web Control for Projector Products

Vulnerability Reference: CVE-2025-64310

Thank you for your using Epson products.

A vulnerability has been identified in some Epson projector products when using the software (EPSON WebConfig / Epson Web Control *1) that allows you can check the status of the product itself or change settings via a Web browser.

*1 EPSON WebConfig / Epson Web Control allows the user to check the status of the product or change the settings by entering the IP address of the product in the URL field on a web browser such as Microsoft Edge or Safari.

- Confirmed vulnerabilities

The password authentication (Web Control Password and Remote Password) of the affected product does not have a restriction or lockout mechanism, so an attacker can try an unlimited number of passwords, making the projector vulnerable to brute-force attacks. If the Web Control Password or Remote Password are discovered through the brute-force attack, a third party may be able to take control of the projector.

- Operation of turning on-off the projector, input source change etc.
- Editing content stored on a USB flash drive or SD card. (Content Playback mode compatible models)
- Capturing projected images using Remote Camera Access. (Remote Camera Access compatible models)
- Refer to projector’s log file saved on a USB flash drive. (Log Save compatible models)

- Impact of vulnerability

Currently, there are no reports of any attacks exploiting this vulnerability.

- Target products and countermeasures

- Products other than those listed in the attached file are not affected as they either do not contain the vulnerabilities or measures have been taken at the time of shipment.
- For products that are currently on sale, we plan to release countermeasure firmware as shown in the attached file. After the firmware is released and products for which the firmware has been released, we strongly recommend that you download it from the Epson website and apply the update.
- For products for which firmware will be released in the future or for which no measure firmware is scheduled to be provided, we strongly recommend that you take measures by “Workaround method”.

- Workaround method

- Installation and configuration according to the user’s guide

The product should not be directly connected to the Internet and should be installed in a network protected by a firewall. In that case, please set a private IP address and operate.

Set the Web Control Password and Remote Password for each product.

The Web Control Password and Remote Password should be a complex string that is difficult for others to guess, such as mixing not only English characters but also symbols and numbers to make it 8 characters or more.

- Stronger workaround – Block HTTP (TCP/80 port and TCP/443 port) access to the product

After configuring the product, block HTTP access (TCP/80 port and TCP443 port) to the product with a network device (router or switch). Open the port only when you need to update the application settings or firmware.

* Due to blockage, the functions in EPSON WebConfig and Epson Web Control may not be available.

Below is the list of Affected Models:

LS9000B, L890E, L790SE, L890U, L790U, L690U, L790SU, L690SU, L690SE, W55, FH54, 994F, W56S, QB1000B, PQ2010B, PQ2213B, PQ2220B, 810E, L210SF, L210SW, 770Fi, 770F, 760Wi, 760W, L260F, L210W, CO-FH01, CO-W01, PU2220B, PU2216B, PU2213B, LS12000B, PU1008B, PU1007B, PU2010B, L730U, L630U, L530U, L630SU, L30000U, L200F, L200W, L200SW, 735Fi, 725Wi, 725W, 735F, W06, FH06, FH52, TW740, TW750, X49, W49, 972, 982W, 992F, 1485Fi, 800F, 1781W, 1795F, 695Wi, 685Wi, 675Wi, 685W, 675W, 2265U, 2245U, 2165W, 2155W, 2065, 2055, 2040, EV-110, EV-115, ELPWP20, L770U, L570U, LS500B, L1075U, L1065U, L20000U, TW7100, TW9400, L610U, L510U, L610W, EV-100, EV-105, L1755U NL, L1505UH NL, L1755U NL, L1495U, X39, 108, 109W, 970, 980W, 990U, 2042, 2142W, 2247U, 1470Ui, 700U, TW5650, X05, W05, U05, S41, X41, W41, TW650, 5530U, 5520W, 5510, L25000U, 1460Ui, LS10050, L1505U, TW6700, TW8300, L1200U, L1405U, G7905U, G7000W, G7100, X04, W04, S31, X31, U32, X36, 4770W, G6970WU, G6870, G6570WU, G6270W, G6070W, G6170, 965H, 955WH, 945H, X30, W29, X29