SSA-284765: Vulnerability in SIEMENS-branded IP-based CCTV Cameras

Publication Date 2016-11-16
Last Update 2016-11-16
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

The latest update for SIEMENS-branded IP-based CCTV cameras fixes a vulnerability that could allow a remote attacker to obtain administrative credentials from the integrated web server.

Vanderbilt Industries acquired the SIEMENS IP Cameras business in June 2015 and released updates for the affected camera models under the SIEMENS brand.

AFFECTED PRODUCTS

- CCMW3025: All versions < 1.41_SP18_S1
- CVMW3025-IR: All versions < 1.41_SP18_S1
- CFMW3025: All versions < 1.41_SP18_S1
- CCPW3025: All versions < 0.1.73_S1
- CCPW5025: All versions < 0.1.73_S1
- CCMD3025-DN18: All versions < v1.394_S1
- CCID1445-DN18: All versions < v2635
- CCID1445-DN28: All versions < v2635
- CCID1445-DN36: All versions < v2635
- CFIS1425: All versions < v2635
- CCIS1425: All versions < v2635
- CFMS2025: All versions < v2635
- CCMS2025: All versions < v2635
- CVMS2025-IR: All versions < v2635
- CFMW1025: All versions < v2635
- CCMW1025: All versions < v2635

DESCRIPTION

The SIEMENS-branded IP-based CCTV cameras portfolio includes a range of megapixel cameras in various configuration and mounting options.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The

environmental score should therefore be individually assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2016-9155)

An attacker with network access to the web server could obtain administrative credentials by sending certain requests.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

SOLUTION

Vanderbilt has released the following updates. Siemens encourages customers to upgrade to the new versions as soon as possible:

- CCMW3025: Update to 1.41_SP18_S1 [1]
- CVMW3025-IR: Update to 1.41_SP18_S1 [2]
- CFMW3025: Update to 1.41_SP18_S1 [3]
- CCPW3025: Update to 0.1.73_S1 [4]
- CCPW5025: Update to 0.1.73_S1 [5]
- CCMD3025-DN18: Update to v1.394_S1 [6]
- CCID1445-DN18: Update to v2635 [7]
- CCID1445-DN28: Update to v2635 [8]
- CCID1445-DN36: Update to v2635 [9]
- CFIS1425: Update to v2635 [10]
- CCIS1425: Update to v2635 [11]
- CFMS2025: Update to v2635 [12]
- CCMS2025: Update to v2635 [13]
- CVMS2025-IR: Update to v2635 [14]
- CFMW1025: Update to v2635 [15]
- CCMW1025: Update to v2635 [16]

Until patches can be applied, restricting access to the integrated web server with appropriate mechanisms is recommended.

As a general security measure, Siemens recommends to operate the devices within trusted networks, and to protect network access to the devices with appropriate mechanisms. Siemens also recommends enabling authentication on the web server.

ADDITIONAL RESOURCES

[1] Firmware update for CCMW3025 can be obtained here: https://is.spiap.com/products/video/1_cameras/11_ip_camerars/box_cameras/ccmw3025.html

[2] Firmware update for CVMW3025-IR can be obtained here: https://is.spiap.com/products/video/1_cameras/11_ip_camerars/114_vandal_resistent_dome_cameras/cvmw3025-ir.html

[3] Firmware update for CFMW3025 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/112_fixed_dome_cameras/cfmw3025.html

[4] Firmware update for CCPW3025 can be obtained here:
https://qa.spiap.com/products/video/1_cameras/11_ip_camerars/bullet-kameror/ip-bullet-camera.html

[5] Firmware update for CCPW5025 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/bullet-kameror/ccpw5025-ir.html

[6] Firmware update for CCMD3025-DN18 can be obtained here:
https://qa.spiap.com/products/video/1_cameras/11_ip_camerars/113_speeddome_cameras/ccmd3025.html

[7] Firmware update for CCID1445-DN18 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/113_speeddome_cameras/ccid1445dn18.html

[8] Firmware update for CCID1445-DN28 can be obtained here:
https://qa.spiap.com/products/video/1_cameras/11_ip_camerars/113_speeddome_cameras/ccid1445dn26.html

[9] Firmware update for CCID1445-DN36 can be obtained here:
https://qa.spiap.com/products/video/1_cameras/11_ip_camerars/113_speeddome_cameras/ccid1445dn36.html

[10] Firmware update for CFIS1425 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/112_fixed_dome_cameras/cfis1425.html

[11] Firmware update for CCIS1425 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/box_cameras/ccis1425.html

[12] Firmware update for CFMS2025 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/112_fixed_dome_cameras/cfms2025.html

[13] Firmware update for CCMS2025 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/box_cameras/ccms2025.html

[14] Firmware update for CVMS2025-IR can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/114_vandal_resistent_dome_cameras/cvms2025ir.html

[15] Firmware update for CFMW1025 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/112_fixed_dome_cameras/cfmw1325.html

[16] Firmware update for CCMW1025 can be obtained here:
https://is.spiap.com/products/video/1_cameras/11_ip_camerars/box_cameras/ccmw1325.html

[17] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-11-16): Publication Date

DISCLAIMER