Published:2026/04/20 Last Updated:2026/04/20

JVNVU#94271449
Multiple vulnerabilities in silex technology SD-330AC and AMC Manager

JVN
HOME
What is JVN ?
Instructions
List of Vulnerability Report
VN_JP
VN_JP(Unreachable)
VN_VU
TA
TRnotes
JVN iPedia
MyJVN
JVNJS/RSS
Vendor List
List of unreachable developers
Contact

Overview

SD-330AC and AMC Manager provided by silex technology, Inc. contain multiple vulnerabilities.

Products Affected

- SD-330AC Ver.1.42 and earlier
- AMC Manager Ver.5.0.2 and earlier

Description

SD-330AC and AMC Manager provided by silex technology, Inc. contain multiple vulnerabilities listed below.

- **Stack-based buffer overflow in processing the redirect URLs (CWE-121)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score 8.7
  - CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Base Score 8.8
  - CVE-2026-32955

- **Heap-based buffer overflow in processing the redirect URLs (CWE-122)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N Base Score 9.3
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score 9.8
  - CVE-2026-32956

- **Missing authentication for critical function on firmware maintenance (CWE-306)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Base Score 6.9
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N Base Score 5.3
  - CVE-2026-32957

- **Use of hard-coded cryptographic key (CWE-321)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N Base Score 6.9
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N Base Score 6.5

- CVE-2026-32958

- **Use of a broken or risky cryptographic algorithm (CWE-327)**
  - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N Base Score 8.2
  - CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 5.9
  - CVE-2026-32959

- **Sensitive information in resource not removed before reuse (CWE-226)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N Base Score 7.1
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N Base Score 6.5
  - CVE-2026-32960

- **Heap-based buffer overflow in packet data processing of sx_smpd (CWE-122)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N Base Score 6.9
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score 5.3
  - CVE-2026-32961

- **Missing authentication for critical device setting function (CWE-306)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Base Score 6.9
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N Base Score 5.3
  - CVE-2026-32962

- **Reflected cross-site scripting (CWE-79)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N Base Score 5.1
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score 6.1
  - CVE-2026-32963

- **CRLF injection (CWE-93)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N Base Score 6.9
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L Base Score 6.5
  - CVE-2026-32964

- **Initialization of a resource with an insecure default (CWE-1188)**
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N Base Score 8.7
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score 7.5
  - CVE-2026-32965

- **Dependency on vulnerable third-party component (CWE-1395)**

    - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N Base Score 8.7
    - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score 7.5
    - CVE-2015-5621

- **Incorrect privilege assignment (CWE-266)**
    - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N Base Score 6.9
    - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score 5.3
    - CVE-2024-24487

Impact

- Arbitrary code may be executed on the device (CVE-2026-32955, CVE-2026-32956)
- Arbitrary file may be uploaded on the device without authentication (CVE-2026-32957)
- An administrative user may be directed to apply a fake firmware update (CVE-2026-32958)
- Information in the traffic may be retrieved via man-in-the-middle attack (CVE-2026-32959)
- An attacker may login to the device without knowing the password by sending a crafted packet (CVE-2026-32960)
- Processing a crafted packet may cause a temporary denial-of-service (DoS) condition (CVE-2026-32961)
- The device configuration may be altered without authentication (CVE-2026-32962)
- When a user logs in to the affected device and access some crafted web page, arbitrary script may be executed on the user's browser (CVE-2026-32963)
- Processing some crafted configuration data may lead to arbitrary entries injected to the system configuration (CVE-2026-32964)
- When the affected device is connected to the network with the initial (factory-default) configuration, the device can be configured with the null string password (CVE-2026-32965)
- The old vulnerable version of net-snmp programs embedded in the device can be exploited by crafted packets, causing a denial-of-service (DoS) condition (CVE-2015-5621)
- No authentication is required to reboot the affected device (CVE-2024-24487)

Solution

Update the Firmware

Update the firmware to the latest version according to the information provided by the developer.
The developer has released the following versions to address this vulnerability.

- SD-330AC firmware Ver.1.50 or later
- AMC Manager Ver.5.1.0 or later

Apply the Workaround

CVE-2026-32955, CVE-2026-32956, CVE-2026-32957, CVE-2026-32963

Disable HTTP/HTTPS service.

CVE-2026-32958, CVE-2026-32965

Set a password for the settings web interface.

CVE-2015-5621

Disable SNMP service.

Vendor Status

Vendor	Link
silex technology, Inc.	Multiple Vulnerabilities in SD-330AC

References

JPCERT/CC Addendum

Vulnerability Analysis by JPCERT/CC

Credit

Francesco La Spina of Forescout Technologies reported these vulnerabilities to CISA ICS.
At the request of CISA ICS, JPCERT/CC coordinated with the developer.

Other Information

JPCERT Alert	
JPCERT Reports	
CERT Advisory	
CPNI Advisory	
TRnotes	
CVE	CVE-2026-32955
	CVE-2026-32956
	CVE-2026-32957
	CVE-2026-32958
	CVE-2026-32959
	CVE-2026-32960
	CVE-2026-32961
	CVE-2026-32962

	CVE-2026-32963
	CVE-2026-32964
	CVE-2026-32965
JVN iPedia	