

Forum:[Hack Forums](#)

Thread: [CyberData 011209 SIP Emergency Intercom](#)

Stanley - June 18, 2025, 2:05 pm

CyberData 011209 SIP Emergency Intercom

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 9.3

ATTENTION: Exploitable remotely/low attack complexity

Vendor: CyberData

Equipment: 011209 SIP Emergency Intercom

Vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Missing Authentication for Critical Function, SQL Injection, Insufficiently Protected Credentials, Path Traversal: '.../.../'

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to disclose sensitive information, cause a denial-of-service condition, or achieve code execution.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following CyberData products are affected:

011209 SIP Emergency Intercom: Versions prior to 22.0.1

3.2 VULNERABILITY OVERVIEW

3.2.1 Authentication Bypass Using an Alternate Path or Channel CWE-288

011209 Intercom could allow an unauthenticated user access to the Web Interface through an alternate path.

CVE-2025-30184 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2025-30184. A base score of 9.3 has been calculated; the CVSS vector string is

(AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N).

3.2.2 Missing Authentication for Critical Function CWE-306

011209 Intercom exposes features that could allow an unauthenticated to gain access and cause a denial-of-service condition or system disruption.

CVE-2025-26468 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

A CVSS v4 score has also been calculated for CVE-2025-26468. A base score of 8.7 has been calculated; the CVSS vector string is

(AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N).

3.2.3 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-89

011209 Intercom could allow an unauthenticated user to gather sensitive information through blind SQL injections.

CVE-2025-30507 has been assigned to this vulnerability. A CVSS v3.1 base score of 5.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

A CVSS v4 score has also been calculated for CVE-2025-30507. A base score of 6.9 has been

calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N).

3.2.4 Insufficiently Protected Credentials CWE-522

011209 Intercom does not properly store or protect web server admin credentials.

CVE-2025-30183 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

A CVSS v4 score has also been calculated for CVE-2025-30183. A base score of 8.7 has been calculated; the CVSS vector string is

(AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N).

3.2.5 Path Traversal: '.../.../' CWE-35

011209 Intercom could allow an authenticated attacker to upload arbitrary files to multiple locations within the system.

CVE-2025-30515 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2025-30515. A base score of 9.3 has been calculated; the CVSS vector string is

(AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Communications, Emergency Services, Commercial Facilities

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: United States

3.4 RESEARCHER

Vera Mens of Claroty Team82 reported these vulnerabilities to CISA.

4. MITIGATIONS

CyberData recommends users update to v22.0.1

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social

engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

5. UPDATE HISTORY

June 5, 2025: Initial Publication

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-155-01>