ARMIS LABS

Report

Frostbyte10

How To Mitigate Ten Vulnerabilities Impacting Mission-Critical Equipment

Executive Summary

Armis Labs identified ten vulnerabilities affecting Copeland E2 and E3 controllers, devices that are integral to managing critical building and refrigeration systems, including compressor groups, condensers and walk-in units, HVAC and lighting systems.

Collectively, Armis named them **“Frostbyte10”** and worked with Copeland to investigate these findings, understand the underlying issues, and work towards a resolution.

Today, updated Copeland firmware is available and we recommend patching affected devices to ensure the vulnerabilities are addressed promptly.

The flaws discovered could have allowed unauthorized actors to remotely manipulate parameters, disable systems, execute remote code, or gain unauthorized access to sensitive operational data. When combined and exploited, these vulnerabilities can result in unauthenticated remote code execution with root privileges.

Their potential impact directly threatens physical infrastructure, food safety, the supply chain, and society:

- Food can spoil or become unsafe if refrigeration control is lost.
- Goods can be contaminated if refrigeration is disabled or tampered with.
- Lighting systems could fail to activate in an emergency.
- Cold chain logistics and cooling systems could be rendered inoperable.

The retail sector is facing heightened scrutiny due to a significant increase in sophisticated cyberattacks. This global expansion places retailers directly in the crosshairs, signaling an urgent and escalating threat. The Copeland E2 and E3 controller vulnerabilities discovered by Armis Labs represented a potential high-value target for attackers seeking to disrupt or ransom retail infrastructure providers.

Due to the severity of these vulnerabilities and the impact, we urge any organization using these controllers to assess their current exposure and to deploy mitigation actions immediately.

Affected Devices

Copeland E2 and E3 supervisory controllers are essentially advanced building management systems designed to streamline operations, improve energy efficiency, and ensure food quality. The E2 platform was the industry standard for many years, while the E3 controller represents more power, better connectivity, and a more user-friendly experience compared to its predecessor.

More information about the affected devices can be found on the vendor website:

- Copeland E2 Facility Management System
- Copeland E3 Supervisory Control

Key Findings and Vulnerabilities

#	Vulnerability	Description	Base Severity	Base Score	Vector String
CVE-2025-6519	Consistent predictable generation of the password for the default application service admin user “ONEDAY”	E3 Site Supervisor Control (firmware version < 2.31F01) has a default admin user “ONEDAY” with a daily generated password. An attacker can predictably generate the password for the ONEDAY user. The ONEDAY user cannot be deleted or modified by any user.	CRITICAL	9.3	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:L/SA:L
CVE-2025-52543	Login to the application services using only the password hash	E3 Site Supervisor Control (firmware version < 2.31F01) application services (MGW and RCI) uses client side hashing for authentication. An attacker can authenticate by obtaining only the password hash.	MEDIUM	5.3	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:L/SA:L
CVE-2025-52544	Arbitrary read file from the filesystem	E3 Site Supervisor Control (firmware version < 2.31F01) has a floor plan feature that allows for an unauthenticated attacker to upload floor plan files. By uploading a specially crafted floor plan file, an attacker can access any file from the E3 file system	HIGH	8.8	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N
CVE-2025-52545	Privilege escalation in the application services	E3 Site Supervisor Control (firmware version < 2.31F01) RCI service contains an API call to read users info, which returns all usernames and password hashes for the application services.	HIGH	7.7	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:L/SA:L

Key Findings and Vulnerabilities

#	Vulnerability	Description	Base Severity	Base Score	Vector String
CVE-2025-52546	Stored XSS by uploading a specially crafted floor plan file	E3 Site Supervisor Control (firmware version < 2.31F01) has a floor plan feature that allows for an unauthenticated attacker to upload floor plan files. By uploading a specially crafted floor plan file, an attacker can inject a stored XSS to the floorplan web page.	MEDIUM	5.1	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CVE-2025-52547	DoS to the application services	E3 Site Supervisor Control (firmware version < 2.31F01) MGW service contains an API call that lacks input validation. An attacker can use this command to continuously crash the application services.	HIGH	8.7	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
CVE-2025-52548	Enabling SSH and Shellinabox on the vulnerable machine	E3 Site Supervisor Control (firmware version < 2.31F01) contains a hidden API call in the application services that enables SSH and Shellinabox, which exist but are disabled by default. An attacker with admin access to the application services can utilize this API to enable remote access to the underlying OS.	MEDIUM	6.9	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
CVE-2025-52549	Predictable root linux password generation	E3 Site Supervisor Control (firmware version < 2.31F01) generates the root linux password on each boot. An attacker can generate the root linux password for a vulnerable device based on known or easy to fetch parameters.	CRITICAL	9.2	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:L/SA:L

Key Findings and Vulnerabilities

#	Vulnerability	Description	Base Severity	Base Score	Vector String
CVE-2025-52550	Firmware upgrade packages are unsigned	E3 Site Supervisor Control (firmware version < 2.31F01) firmware upgrade packages are unsigned. An attacker can forge malicious firmware upgrade packages. An attacker with admin access to the application services can install a malicious firmware upgrade.	HIGH	8.6	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:L/SA:L
CVE-2025-52551	Proprietary protocol allows for unauthenticated file operations	E2 Facility Management Systems use a proprietary protocol that allows for unauthenticated file operations on any file in the file system.	CRITICAL	9.3	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:L/SA:L

Remediation and Mitigation

If not done yet, organizations using E2 and E3 devices should assess their exposure to these vulnerabilities and take action to implement mitigations:

Copeland E2E controllers have been declared End of Life since October 2024. Affected customers are encouraged to migrate from the E2 to the E3 platform.

Mitigations are available as from the Copeland firmware version 2.31F01. We recommend patching affected devices to ensure the vulnerabilities are addressed promptly.

For more information please refer to Copeland:

- Copeland Product End-of-Life (EOL) Notification
- Copeland E3 Firmware updates

Best Practices and Recommendations

Conduct a Comprehensive Risk Assessment: organizations should assess their use of devices like the E2 and E3 controllers. Conducting a thorough risk assessment will help identify vulnerable systems and prioritize mitigations.

Segmentation and Network Isolation: segregate OT systems from traditional IT networks to limit the exposure of critical infrastructure. Use firewalls and network segmentation to restrict access to critical devices and control systems.

Review and Monitor Remote Access Capabilities: disable or restrict unnecessary remote access capabilities, especially those that are unauthenticated. Ensure default accounts are updated, and strong passwords are used. Monitor remote access logs for suspicious activity and implement strict access control mechanisms.

Security Audits, Vulnerability Scanning and Patching: regularly conduct security audits and vulnerability scans on connected devices and systems. Leverage automated tools to continuously assess security posture and address emerging threats.

Prepare and Test Incident Response Capabilities: Identify critical infrastructure such as OT systems and have a plan in place to identify and contain a cyber attack against such systems with the goal of compromise eradication and rapid recovery.

Employee Training and Awareness: educate employees about the risks associated with cybersecurity and the importance of following security protocols. Create a culture of security awareness across the organization, especially for those handling critical infrastructure.

Collaboration with Security Vendors: engage with trusted security vendors, like Armis, to stay updated on the latest threats and best practices. Leverage threat intelligence and security research to bolster the organization's security defenses.

ARMIS LABS

About Armis Labs

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape. With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the threats that matter most, right now.

Armed with access to over 6 billion profiled assets and state-of-the-art tools and methodologies, the team at Armis Labs conducts in-depth analyses of evolving threats both in the pre-emergence stage and "in the wild" stage of an attack.

References

Armis Vulnerability Intelligence Database

CVE™ Program Mission

ARMIS®

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform

Industries

Solutions

Resources

Blog

Try Armis

Demo