contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Emerson Ovation: new CVE

CVE-2022-29966 · record published 3 November 2026

Analysis Report

Any site running Emerson Ovation should act now: the record scores this 9.8 (Critical, CVSS 3.1) and no login is required to attack it. The first step is to confirm whether Ovation is reachable from …

PREPARED BY	NamiQ	DATE	3 November 2026
FACTS AS OF	3 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/emerson-ovation-cve-2022-29966

The bottom line

> *Any site running Emerson Ovation should act now: the record scores this 9.8 (Critical, CVSS 3.1) and no login is required to attack it. The first step is to confirm whether Ovation is reachable from any untrusted network segment and to contact Emerson for patch status, as no source names a confirmed fixed version.*

At a glance

Fact	Detail
Product	Emerson Ovation (CVE-2022-29966)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by Icscert on 3 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 3 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Teams operating Emerson Ovation industrial control systems, particularly where the Ovation control network can be reached from a corporate IT segment, a vendor connection, or any other untrusted host.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Emerson Ovation?	Nothing to do for this CVE.	Check the version and network exposure (next questions).
Is your Ovation version before 3.8.0 Feature Pack 1, or at 3.8.0 Feature Pack 3?	Your version may not be in the affected range; confirm with your vendor.	Check who can reach the Ovation control network (next question).
Can any untrusted host reach the Ovation control network?	Exposure is reduced; still seek vendor guidance on patching.	Restrict access immediately and contact Emerson for a fixed version.

What it is

Several protocols in Emerson Ovation carry no authentication at all. The record says an attacker who can reach the system over a network could change controller configuration or force a denial-of-service condition without any credentials.

Why it matters

CWE-306 — missing authentication for a critical function — means no credential stands between an attacker and the ability to send commands to the controller. For a control system, changing controller configuration can alter physical processes; a denial-of-service condition can interrupt monitoring or control entirely. Our reading is that authentication gaps across multiple protocols widen the attack surface considerably: every reachable protocol is a separate path in, not a single point to block. The record was published by ICS-CERT, which is specific to operational technology environments.

Things people will get wrong

- Our Ovation network is air-gapped, so we are safe The record does not condition the flaw on internet access. An air gap reduces exposure but must be confirmed as genuine and actively monitored before concluding no action is needed.
- Version 3.8.0 Feature Pack 1 is the confirmed fix The record lists versions before 3.8.0 FP1 as affected and also lists 3.8.0 FP3 as affected. No source names a confirmed fixed version; seek guidance from Emerson directly.
- A CVSS score of 9.8 means this is already being exploited The score reflects potential impact, not observed exploitation. This record is new and was not on CISA's exploited vulnerabilities list when read.

How we would triage it

This is our judgement.

Step 1: Find the Ovation version you run

- Check the Ovation configuration manager or the system about screen for the installed version number and feature pack identifier.
- Confirm whether the version falls in the affected ranges stated in the record: before 3.8.0 Feature Pack 1, or at 3.8.0 Feature Pack 3.

Step 2: Map who can reach the Ovation control network

- Review firewall rules and network diagrams to confirm whether any untrusted host, corporate IT segment, or external vendor connection can initiate traffic to Ovation systems.
- Verify that network segmentation is enforced at the boundary device, not only documented in a diagram.

Step 3: Restrict untrusted access while awaiting a patch

- Block traffic from untrusted segments to Ovation systems at the network boundary until Emerson confirms a fixed version.
- No source names a fixed version; contact Emerson or your system integrator to obtain patch status and a confirmed release timeline.

Step 4: Confirm the fix when a patched version is available

- When Emerson provides a patched release, verify the installed version matches what the vendor states as fixed before reconnecting the system to wider network segments.
- Document the installed version and the date it was verified.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are reviewing CVE-2022-29966 affecting Emerson Ovation. The record scores this 9.8 (Critical, CVSS 3.1): several Ovation protocols carry no authentication, letting a network attacker change controller configuration or cause a denial-of-service condition. Affected versions listed in the record are: before 3.8.0 Feature Pack 1, and 3.8.0 Feature Pack 3. No source we have read names a confirmed fixed version. Please confirm whether we run Ovation, which version is installed, whether it is reachable from any untrusted network segment, and what patch or workaround Emerson has issued. We would like written confirmation of the installed version, patch status, and any network isolation measures in place within five working days.*

The weakness behind it

The record classes this as CWE-306.

The sources, in their words

The CVE record:

> *Emerson Ovation has several protocols that have no authentication, which could allow an attacker to change controller configuration or cause a denial-of-service condition.*

Versions of Emerson Ovation the record lists as affected:

- all versions up to, but not including, Version 3.8.0 Feature Pack 1
- 3.8.0 Feature Pack 3

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2022-29966
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2022-29966
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- No vendor advisory was available; the confirmed fixed version and any official workaround are not stated in the record.
- Which specific Ovation protocols lack authentication is not named in the record.
- Whether the flaw is exploitable over a routed wide-area connection or requires local network access is not stated.
- Whether any compensating control at the protocol or network layer reduces exposure is not addressed in the record.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 3 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2022-29966: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
3 November 2026	CVE record published by Icscert.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Ovation on an affected version reachable from a corporate IT network or external vendor link	High	Immediately — isolate the network segment before patching
Ovation version unknown and network segmentation unconfirmed	High	This week — establish version and exposure before deciding next steps
Ovation on an affected version with firewall rules in place but not recently verified	High	This week — verify segmentation is enforced, not just documented
Ovation air-gapped and on an affected version with no untrusted path confirmed	Medium	Next maintenance window — patch when a fixed version is confirmed
Not running Emerson Ovation	None	None for this CVE

Appendix 4. Definition of done

- Every Emerson Ovation you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2022-29966: https://www.cve.org/CVERecord?id=CVE-2022-29966
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: www.cisa.gov: https://www.cisa.gov/news-events/ics-advisories/icsa-24-158-02
- Reference in the CVE record: github.com: https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2024/icsa-24-158-02.json