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 up to and including Version 3.8.0 Feature Pack 1 should plan to upgrade; the record scores this 9.8 because no login is needed to reach the affected protocols. Check …

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 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

Correction, 5 November 2026: an earlier version of this note listed 3.8.0 Feature Pack 3 as an affected release and said no source named a fixed version. The CVE record lists 3.8.0 Feature Pack 3 as unaffected, and its remediation text says to upgrade to it. Confirm your installed release and the upgrade path with Emerson before you change a control system.

The bottom line

> *Any site running Emerson Ovation up to and including Version 3.8.0 Feature Pack 1 should plan to upgrade; the record scores this 9.8 because no login is needed to reach the affected protocols. Check which Feature Pack is installed first, then apply Feature Pack 3.*

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. The identifier was reserved on 29 April 2022, so the flaw may be older than the record. Not on CISA's list of exploited vulnerabilities when we read it on 5 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	Emerson Ovation 3.8.0 Feature Pack 3, as stated in the CVE record.
Who looks first	Engineers and administrators responsible for Emerson Ovation controllers running Version 3.8.0 Feature Pack 1 or any earlier release.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you operate any Emerson Ovation controllers?	Nothing to do for this CVE.	Check the installed version and Feature Pack (next question).
Is the installed version 3.8.0 Feature Pack 1 or earlier?	The record lists Feature Pack 3 as unaffected; confirm and stop.	Assess whether untrusted hosts can reach the Ovation control network.
Can any untrusted host reach the Ovation control network segment?	Upgrade is still recommended; treat as medium priority.	Treat as high priority; begin upgrade planning immediately.

What it is

The record says several Ovation protocols carry no authentication check. Anyone who can reach those protocols across the network can send commands to reconfigure a controller or cause it to stop responding.

Why it matters

CWE-306 — missing authentication for a critical function — means the gap is in the protocol design, not a configuration mistake. An attacker already on the control network segment needs no password to reconfigure a controller or cause a denial-of-service condition. Our reading is that the 9.8 score reflects the consequence of losing control of physical processes: in an industrial setting, that consequence extends well beyond data loss. The record has not been listed as exploited, but the absence of any authentication makes the attack straightforward for anyone who can reach the network segment.

Things people will get wrong

- Feature Pack 2 must be safe since the record only lists Feature Pack 1 as affected The record names Feature Pack 1 as the last affected version and Feature Pack 3 as unaffected; it says nothing about Feature Pack 2 either way. That gap is listed under what the sources do not say.
- Network segmentation removes the need to upgrade The vendor guidance in the record recommends upgrading regardless of network architecture. Segmentation reduces the attack surface but does not remove the protocol flaw.

How we would triage it

This is our judgement.

Step 1: Find the version and Feature Pack installed

- On each Ovation workstation, check the installed software version and Feature Pack level. The record's affected range is all versions up to and including 3.8.0 Feature Pack 1.

Step 2: Check whether the control network is exposed

- Confirm whether any firewall rule, remote-access connection, or IT–OT bridge allows traffic from untrusted hosts to reach the Ovation control network. The record says protocols have no authentication, so network reach is the deciding factor.

Step 3: Apply Feature Pack 3

- The CVE record names 3.8.0 Feature Pack 3 as the unaffected release. The vendor guidance states it addresses many of the identified vulnerabilities. Coordinate with your Ovation support contact; upgrades require a maintenance window and change management sign-off.

Step 4: Review OCR3000 controllers if the upgrade path is blocked

- The CVE record notes the vendor recommends considering OCR3000 controllers for an extra layer of protection not available to older models. Raise this with your support contact if existing hardware limits the Feature Pack 3 upgrade path.

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, which affects Emerson Ovation up to and including Version 3.8.0 Feature Pack 1. The flaw is that several Ovation protocols carry no authentication, allowing anyone who can reach the control network to reconfigure controllers or cause a denial-of-service condition. The CVE record names Version 3.8.0 Feature Pack 3 as the fix and states it addresses many of the identified vulnerabilities. Please confirm whether we run any Emerson Ovation systems, which version and Feature Pack is currently installed, and whether the control network is isolated from corporate IT and remote-access connections. Please provide written confirmation of the installed version and whether Feature Pack 3 is in place or scheduled, by [date]. Thank you.*

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 and including Version 3.8.0 Feature Pack 1

It lists these as unaffected:

- 3.8.0 Feature Pack 3

What the record says to do about it, in the vendor's words:

> *Emerson recommends the following: • Upgrade to the currently available release of Ovation 3.8.0 Feature Pack 3 for remediation of many of the identified vulnerabilities. • Users are advised to consider the use of OCR3000 controllers, which offer an extra layer of protection that is not available to older controller models. • Deploy and configure Ovation systems and related components as described in the Cybersecurity for Ovation Systems manual (OVREF1000). Ovation Users' Group Website (User Manuals | Reference Manuals) https://www.ovationusers.com/ (login required) • Users with questions or co*

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

- The record does not name which specific Ovation protocols lack authentication.
- Feature Pack 2 is not listed as either affected or unaffected; the record goes from Feature Pack 1 (affected) to Feature Pack 3 (unaffected) with no mention of Feature Pack 2.
- No release date for Feature Pack 3 is given in the record or any source that could be read.
- The record does not say whether hardware that cannot run Feature Pack 3 has a remediation path beyond the OCR3000 recommendation.
- 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 5 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 affected version; control network reachable from corporate IT or any untrusted segment	High	Before the next maintenance window
Ovation on affected version; older controller hardware where the vendor recommends considering OCR3000 migration	High	Raise with support contact immediately
Ovation on affected version; fully air-gapped with no untrusted network access	Medium	Next scheduled patch cycle
Ovation already running Feature Pack 3	None	None for this CVE
No Emerson Ovation in the estate	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