



# Multiple vulnerabilities in MphRx's Minerva

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-5780  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | INCIBE   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-04-28 13:19:22 UTC  |
| <b>Updated</b>         | 2026-05-05 14:22:38 UTC  |
| <b>Description</b>     | An insecure direct object reference (IDOR) vulnerability in MphRx's Minerva V3.6.0, specifically in the endpoint '/minerva/m |

## Risk And Classification

**Primary CVSS:** v4.0 8.5 HIGH from cve-coordination@incibe.es

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000430000 probability, percentile 0.129510000 (date 2026-05-05)

**Problem Types:** CWE-284 | CWE-284 CWE-284 Improper Access Control

| Version | Source                     | Type      | Score | Severity | Vector  |
|---------|----------------------------|-----------|-------|----------|---|
| 4.0     | cve-coordination@incibe.es | Secondary | 8.5   | HIGH     | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA |
| 4.0     | CNA                        | CVSS      | 8.5   | HIGH     | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA |
| 3.1     | nvd@nist.gov               | Primary   | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N                  |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/V:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor       | Product | Version | Update | Edition | Language |
|-------------|--------------|---------|---------|--------|---------|----------|
| Application | Agilonhealth | Minerva | 3.6.0   | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor | Product | Version        | Platforms     |
|--------|--------|---------|----------------|---------------|
| CNA    | MphRx  | Minerva | affected 3.6.0 | Not specified |

## References

| Reference  | Source                     | Link   | Tags            |
|--|----------------------------|--|-----------------|
| <a href="http://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-mphrxs-...">www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-mphrxs-...</a> | cve-coordination@incibe.es | <a href="http://www.incibe.es">www.incibe.es</a> | Third Party Adv |
| CVE Program record   | CVE.ORG                    | <a href="http://www.cve.org">www.cve.org</a>     | canonical       |
| NVD vulnerability detail   | NVD                        | <a href="http://nvd.nist.gov">nvd.nist.gov</a>   | canonical, anal |

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Alejandro Rivera León (en)

## Additional Advisory Data

### Solutions

**CNA:** No solution has been reported yet.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)