



# CVE-2022-28171

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2022-28171  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | hsrc@hikvision.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-06-27 18:15:00 UTC   |
| <b>Updated</b>         | 2023-08-02 17:21:00 UTC   |
| <b>Description</b>     | The web module in some Hikvision Hybrid SAN/Cluster Storage products have the following security vulnerability. Due to th |

## Risk And Classification

### Problem Types: CWE-77

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                                 | Version | Update | Edition | Language |
|------------------|---------------------------|---|---------|--------|---------|----------|
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a71024</a>               | -       | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a71024 Firmware</a>      | All     | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a71024 Firmware</a>      | All     | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a71048</a>               | -       | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a71048r-cvs</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a71048r-cvs Firmware</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a71048 Firmware</a>      | All     | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a71072r</a>              | -       | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a71072r Firmware</a>     | All     | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a72024</a>               | -       | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a72024 Firmware</a>      | All     | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a72024 Firmware</a>      | All     | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a72048r-cvs</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a72048r-cvs Firmware</a> | All     | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a72072r</a>              | -       | All    | All     | All      |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a72072r Firmware</a>     | All     | All    | All     | All      |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a80316s</a>              | -       | All    | All     | All      |

|                  |                           |                                     |     |     |     |     |
|------------------|---------------------------|-------------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a80316s Firmware</a> | All | All | All | All |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a80624s</a>          | -   | All | All | All |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a80624s Firmware</a> | All | All | All | All |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a81016s</a>          | -   | All | All | All |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a81016s Firmware</a> | All | All | All | All |
| Hardware         | <a href="#">Hikvision</a> | <a href="#">Ds-a82024d</a>          | -   | All | All | All |
| Operating System | <a href="#">Hikvision</a> | <a href="#">Ds-a82024d Firmware</a> | All | All | All | All |

## References

| Reference  | Source  | Link   | Tags  |
|--|---------|--|-------|
| Security Vulnerability in Some Hikvision Hybrid SAN Products - Security Advisory - Hikvision | MISC    | <a href="http://www.hikvision.com">www.hikvision.com</a>             |       |
| Hikvision Remote Code Execution / XSS / SQL Injection ≈ Packet Storm                         | MISC    | <a href="http://packetstormsecurity.com">packetstormsecurity.com</a> |       |
| Hikvision Hybrid SAN Ds-a71024 SQL Injection ≈ Packet Storm                                  | MISC    | <a href="http://packetstormsecurity.com">packetstormsecurity.com</a> |       |
| CVE Program record   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                         | canor |
| NVD vulnerability detail   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       | canor |

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Thurein Soe

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

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