



# CVE-2010-3684

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-3684                                                                                                              |
| <b>State</b>           | PUBLISHED                                                                                                                  |
| <b>Assigner</b>        | mitre                                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2010-09-29 17:00:05 UTC                                                                                                    |
| <b>Updated</b>         | 2026-04-29 01:13:23 UTC                                                                                                    |
| <b>Description</b>     | The FTP authentication module in Synology Disk Station 2.x logs passwords to the web application interface in cases of inc |

## Risk And Classification

**Primary CVSS:** v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

**Problem Types:** CWE-255 | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

## NVD Known Affected Configurations (CPE 2.3)

| Type     | Vendor   | Product             | Version | Update | Edition | Language |
|----------|----------|---------------------|---------|--------|---------|----------|
| Hardware | Synology | Disk Station Ds1010 | All     | All    | All     | All      |

|                  |                          |                                        |          |     |     |     |
|------------------|--------------------------|----------------------------------------|----------|-----|-----|-----|
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds109</a>     | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds110j</a>    | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds110</a>     | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds209</a>     | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds210j</a>    | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds210</a>     | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds409slim</a> | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds410</a>     | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds410j</a>    | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds411</a>     | All      | All | All | All |
| Hardware         | <a href="#">Synology</a> | <a href="#">Disk Station Ds710</a>     | All      | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.2-0942 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.2-1041 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.2-1042 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.2-1045 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.3-1139 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.3-1141 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.3-1144 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.3-1157 | All | All | All |
| Operating System | <a href="#">Synology</a> | <a href="#">Dsm</a>                    | 2.3-1161 | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |  |

| References               |                                      |                                       |                     |
|--------------------------|--------------------------------------|---------------------------------------|---------------------|
| Reference                | Source                               | Link                                  | Tags                |
| SecurityFocus            | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.securityfocus.com</a> |                     |
| CVE Program record       | CVE.ORG                              | <a href="#">www.cve.org</a>           | canonical           |
| NVD vulnerability detail | NVD                                  | <a href="#">nvd.nist.gov</a>          | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

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