

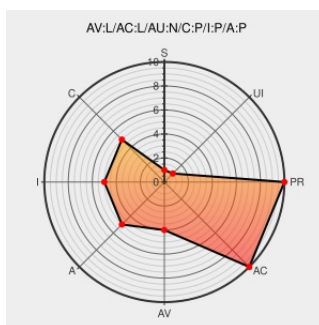


# CVE-2001-1148

Published on: 06/13/2001 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:18 PM UTC

## CVE-2001-1148

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openserver](#) from [Sco](#) contain the following vulnerability:

Multiple buffer overflows in programs used by scoadmin and sysadmsh in SCO OpenServer 5.0.6a and earlier allow local users to gain privileges via a long TERM environment variable to (1) atcronsh, (2) auditsh, (3) authsh, (4) backupsh, (5) lpsh, (6) sysadm.menu, or (7) termsh.

CVE-2001-1148 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

**Access Vector**

**LOCAL**

**Access Complexity**

**LOW**

**Authentication**

**NONE**

**Confidentiality Impact**

**PARTIAL**

**Integrity Impact**

**PARTIAL**

**Availability Impact**

**PARTIAL**

## CVE References

**Description**

**Tags**

**Link**

SecurityFocus

[Patch](#)  
[Vendor Advisory](#)  
[www.securityfocus.com](#)  
[text/html](#)

[CALDERA CSSA-2001-SCO.25](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)  
[text/html](#)

[XF openserver-scoadmin-sysadm-bo\(7281\)](#)

Mailing Lists

[Vendor Advisory](#)  
[www.securityfocus.com](#)  
[text/html](#)

[VULN-DEV 20010613 SCO atcronsh auditsh termsh overflows](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further,

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                            | Vendor | Product    | Version | Update | Edition | Language |
|---------------------------------|--------|------------|---------|--------|---------|----------|
| Operating System                | Sco    | Openserver | All     | All    | All     | All      |
| cpe:2.3:o:sco:openserver:*****: |        |            |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→