



CVE-2011-3849

Published on: 11/18/2011 12:00:00 AM UTC

Last Modified on: 04/08/2021 01:30:00 PM UTC

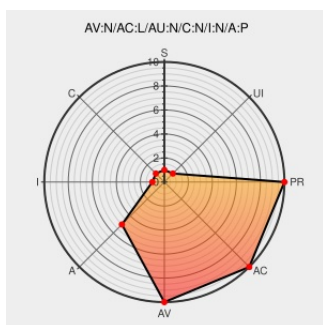
CVE-2011-3849

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Directory](#) from [Broadcom](#) contain the following vulnerability:

Unspecified vulnerability in dxserver before 6279 in CA Directory 8.1 and CA Directory r12 before SP7 CR1 allows remote attackers to cause a denial of service (daemon crash) via a crafted SNMP packet.

CVE-2011-3849 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

404 Not Found

[Patch](#)
[Vendor Advisory](#)
[support.ca.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=%7b286545DB-00B9-4B4C-8DE7-F00827F3CC75%7d](#)

SecurityFocus

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

[BUGTRAQ 20111116 CA20111116-01: Security Notice for CA Directory](#)

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](#).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Directory	8.1	All	All	All
Application	Broadcom	Directory	r12	sp1	All	All
Application	Broadcom	Directory	r12	sp2	All	All
Application	Broadcom	Directory	r12	sp3	All	All
Application	Broadcom	Directory	r12	sp4	All	All
Application	Broadcom	Directory	r12	sp5	All	All
Application	Broadcom	Directory	r12	sp6	All	All
Application	Broadcom	Directory	r12	sp7	All	All
Application	Ca	Directory	8.1	All	All	All
Application	Ca	Directory	r12	sp1	All	All
Application	Ca	Directory	r12	sp2	All	All
Application	Ca	Directory	r12	sp3	All	All
Application	Ca	Directory	r12	sp4	All	All
Application	Ca	Directory	r12	sp5	All	All
Application	Ca	Directory	r12	sp6	All	All
Application	Ca	Directory	r12	sp7	All	All
Application	Ca	Directory	8.1	All	All	All
Application	Ca	Directory	r12	sp1	All	All
Application	Ca	Directory	r12	sp2	All	All
Application	Ca	Directory	r12	sp3	All	All
Application	Ca	Directory	r12	sp4	All	All
Application	Ca	Directory	r12	sp5	All	All
Application	Ca	Directory	r12	sp6	All	All
Application	Ca	Directory	r12	sp7	All	All

```
cpe:2.3:a:broadcom:directory:8.1.*.*.*.*.*.*:
```

```
cpe:2.3:a:broadcom:directory:r12:sp1:*:*:*:*:
```

```
cpe:2.3:a:broadcom:directory:r12:sp2:*:*:*:*:*
```

```
cpe:2.3:a:broadcom:directory:r12:sp3:*:*:*:*:
```

```
cpe:2.3:a:broadcom:directory:r12:sp4:*:*:*:*:
```

```
cpe:2.3:a:broadcom:directory:r12:sp5:*:*:*:*:*:
```

cpe:2.3:a:broadcom:directory:r12:sp6:*****:
cpe:2.3:a:broadcom:directory:r12:sp7:*****:
cpe:2.3:a:ca:directory:8.1:*****:
cpe:2.3:a:ca:directory:r12:sp1:*****:
cpe:2.3:a:ca:directory:r12:sp2:*****:
cpe:2.3:a:ca:directory:r12:sp3:*****:
cpe:2.3:a:ca:directory:r12:sp4:*****:
cpe:2.3:a:ca:directory:r12:sp5:*****:
cpe:2.3:a:ca:directory:r12:sp6:*****:
cpe:2.3:a:ca:directory:r12:sp7:*****:
cpe:2.3:a:ca:directory:8.1:*****:
cpe:2.3:a:ca:directory:r12:sp1:*****:
cpe:2.3:a:ca:directory:r12:sp2:*****:
cpe:2.3:a:ca:directory:r12:sp3:*****:
cpe:2.3:a:ca:directory:r12:sp4:*****:
cpe:2.3:a:ca:directory:r12:sp5:*****:
cpe:2.3:a:ca:directory:r12:sp6:*****:
cpe:2.3:a:ca:directory:r12:sp7:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)