



# CVE-2006-0306

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

## Summary

<b>CVE</b>	CVE-2006-0306
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-01-19 00:03:00 UTC
<b>Updated</b>	2021-04-13 20:13:00 UTC
<b>Description</b>	The DM Primer (dmprimer.exe) in the DM Deployment Common Component in Computer Associates (CA) BrightStor Mobil

## Risk And Classification

**Problem Types:** CWE-399

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.0	All	All	All
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.1	All	All	All
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.1	sp1	All	All
Application	Broadcom	Brightstor Mobile Backup	r4.0	All	All	All
Application	Broadcom	Business Protection Suite	2.0	All	All	All
Application	Broadcom	Desktop Protection Suite	2.0	All	All	All
Application	Broadcom	Server Protection Suite	2	All	All	All
Application	Broadcom	Unicenter Remote Control	5.2	All	All	All
Application	Broadcom	Unicenter Remote Control	6.0	All	All	All
Application	Broadcom	Unicenter Remote Control	6.0	sp1	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.0	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	sp1	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.0	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	sp1	All	All
Application	Ca	Brightstor Mobile Backup	r4.0	All	All	All

Application	Ca	Brightstor Mobile Backup	r4.0	All	All	All
Application	Ca	Business Protection Suite	2.0	All	All	All
Application	Ca	Business Protection Suite	2.0	All	All	All
Application	Ca	Desktop Protection Suite	2.0	All	All	All
Application	Ca	Desktop Protection Suite	2.0	All	All	All
Application	Ca	Server Protection Suite	2	All	All	All
Application	Ca	Server Protection Suite	2	All	All	All
Application	Ca	Unicenter Remote Control	5.2	All	All	All
Application	Ca	Unicenter Remote Control	6.0	All	All	All
Application	Ca	Unicenter Remote Control	6.0	sp1	All	All
Application	Ca	Unicenter Remote Control	6.0	sp1	All	en
Application	Ca	Unicenter Remote Control	6.0	sp1	All	fr
Application	Ca	Unicenter Remote Control	6.0_build_6.0.56.3	All	All	en
Application	Ca	Unicenter Remote Control	6.0_build_6.0.74	All	All	de
Application	Ca	Unicenter Remote Control	6.0_build_6.0.74	All	All	en
Application	Ca	Unicenter Remote Control	6.0_build_6.0.74	All	All	fr
Application	Ca	Unicenter Remote Control	5.2	All	All	All
Application	Ca	Unicenter Remote Control	6.0	All	All	All
Application	Ca	Unicenter Remote Control	6.0	sp1	All	All
Application	Ca	Unicenter Remote Control	6.0	sp1	All	en
Application	Ca	Unicenter Remote Control	6.0	sp1	All	fr
Application	Ca	Unicenter Remote Control	6.0_build_6.0.56.3	All	All	en
Application	Ca	Unicenter Remote Control	6.0_build_6.0.74	All	All	de
Application	Ca	Unicenter Remote Control	6.0_build_6.0.74	All	All	en
Application	Ca	Unicenter Remote Control	6.0_build_6.0.74	All	All	fr

## References

Reference	Source	Link
SecurityTracker.com Archives - DM Deployment Common Component (DMPrimer) Lets Remote Users Deny Service	SECTRACK	<a href="#">security</a>
Error handling weakness in DM Primer Service	MISC	<a href="#">www.d</a>
SecurityFocus	BUGTRAQ	<a href="#">www.s</a>
CA DM Deployment Common Component DM Primer vulnerabilities	CONFIRM	<a href="#">www3.i</a>
22529	OSVDB	<a href="#">www.o</a>
Secunia - Advisories - CA DM Deployment Common Component Denial of Service	SECUNIA	<a href="#">secunia</a>
SupportConnect - DM Deployment Common Component Security Notice	CONFIRM	<a href="#">suppor</a>

Computer Associates Unicenter Remote Control DM Primer Remote Denial of Service Vulnerability	BID	<a href="#">www.Si</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.vi</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)