



# CVE-2017-3894

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-3894
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@blackberry.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-10 16:29:00 UTC
<b>Updated</b>	2017-07-08 01:29:00 UTC
<b>Description</b>	A stored cross site scripting vulnerability in the Management Console of BlackBerry Unified Endpoint Manager version 12.6

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Blackberry	Enterprise Service	12.0	All	All	All
Application	Blackberry	Enterprise Service	12.0.1	All	All	All
Application	Blackberry	Enterprise Service	12.1	All	All	All
Application	Blackberry	Enterprise Service	12.1.0	All	All	All
Application	Blackberry	Enterprise Service	12.1.1	All	All	All
Application	Blackberry	Enterprise Service	12.2.0	All	All	All
Application	Blackberry	Enterprise Service	12.2.1	All	All	All
Application	Blackberry	Enterprise Service	12.3.0	All	All	All
Application	Blackberry	Enterprise Service	12.3.1	All	All	All
Application	Blackberry	Enterprise Service	12.4.0	All	All	All
Application	Blackberry	Enterprise Service	12.4.1	All	All	All
Application	Blackberry	Enterprise Service	12.5.0	All	All	All
Application	Blackberry	Enterprise Service	12.5.1	All	All	All
Application	Blackberry	Enterprise Service	12.5.2	All	All	All
Application	Blackberry	Enterprise Service	12.0	All	All	All
Application	Blackberry	Enterprise Service	12.0.1	All	All	All
Application	Blackberry	Enterprise Service	12.1	All	All	All

Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.1.0	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.1.1	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.2.0	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.2.1	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.3.0	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.3.1	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.4.0	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.4.1	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.5.0	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.5.1	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Enterprise Service</a>	12.5.2	All	All	All
Application	<a href="#">Blackberry</a>	<a href="#">Unified Endpoint Manager</a>	All	All	All	All

## References

### Reference

[BSRT-2017-004 Vulnerability in UEM Management Console impacts UEM](#)

[BlackBerry UEM Management Console \(BlackBerry Enterprise Server\) Input Validation Flaw Lets Remote Authenticated Users Conduct Cross](#)

[Multiple BlackBerry Products CVE-2017-3894 HTML Injection Vulnerability](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

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](#)