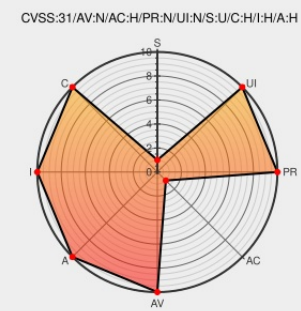
CVE-2009-4011

Published on: 11/08/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:22 PM UTC

CVE-2009-4011

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dtc-xen from Dtc-xen Project contain the following vulnerability:

dtc-xen 0.5.x before 0.5.4 suffers from a race condition where an attacker could potentially get a bash access as xenXX user on the dom0, and then access a potentially reuse an already opened VPS console.

CVE-2009-4011 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2009-4011	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2009-4011
Bug #505072 “Please sync dtc-xen from SID” : Bugs : dtc-	Third Party Advisory	MISC bugs.launchpad.net/ubuntu/+source/dtc-

xen package : Ubuntu	bugs.launchpad.net text/html	xen/+bug/505072
	Product Release Notes tracker.debian.org text/plain	MISC tracker.debian.org/media/packages/d/dtc-xen/changelog-0.5.17-1.1

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	Dtc-xen Project	Dtc-xen	All	All	All	All
Application	Dtc-xen Project	Dtc-xen	All	All	All	All

cpe:2.3:a:dtc-xen_project:dtc-xen:*:*:*:*:*:*:*:*:

cpe:2.3:a:dtc-xen_project:dtc-xen:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/digitalmunition	dtc-xen 0.5.0/0.5.1/0.5.2/0.5.3 privilege escalation [CVE-2009-4011] https://t.co/xSF6jth4K7 https://t.co/7vjICusLDn	2019-11-10 10:28:18

← Previous ID

Next ID→