



CVE-2010-2625

Published on: 07/02/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

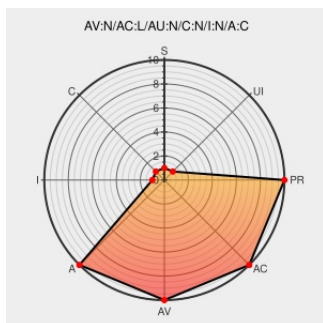
CVE-2010-2625

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Jp1/ Serverconductor / Deployment Manager](#) from [Hitachi](#) contain the following vulnerability:

Unspecified vulnerability in the Client Service for DPM in Hitachi ServerConductor / Deployment Manager 01-00, 01-01, and 06-00 through 06-00-/A; ServerConductor / Deployment Manager Standard Edition and Enterprise Edition 07-50 through 07-55, and 07-57 through 07-59; and JP1/ServerConductor/Deployment Manager Standard and Enterprise Edition 07-50 through 07-56-/F, 08-00 through 08-09-/E, 08-50 through 08-80-/A, 08-06 through 08-07, and 08-51 through 08-70; allows attackers to cause a denial of service (shutdown and reboot) via unknown vectors.

CVE-2010-2625 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

JP1/ServerConductor/Deployment Managerにおける不正にシャットダウン/リブートを実行する問題：ソフトウェア製品セキュリティ情報：ソフトウェア：日立

[Vendor Advisory](#)
[www.hitachi.co.jp](#)
[text/html](#)

[CONFIRM](#)
[www.hitachi.co.jp/Prod/comp/soft1/security/info/vuls/HS10-013/index.html](#)

Hitachi
JP1/ServerConductor/DeploymentManager Denial of Service - Secunia.com

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 40343](#)

No Description Provided

[Exploit](#)
[newdls.com](#)

[OSVDB 65833](#)

Webmail : Solution de messagerie professionnelle
- OVHcloud- OVH

[Patch](#)
[Vendor Advisory](#)
www.vupen.com
[text/html](#)
 VUPEN ADV-2010-1635

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	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-50	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-52	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-56-/f	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-56-/f	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-00	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-00	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-06	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-06	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-07	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-07	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-09-/e	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-09-/e	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-50	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-50	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-51	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-52	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-70	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-70	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-80-/a	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	08-80-/a	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-50	-	standard	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-52	-	enterprise	All
Application	Hitachi	Jp1/ Serverconductor / Deployment Manager	07-56-Vf	-	enterprise	All

[illegible]

[illegible]

Application	Hitachi	Serverconductor / Deployment Manager	07-59	-	enterprise	All
Application	Hitachi	Serverconductor / Deployment Manager	07-59	-	standard	All
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:07-50::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:07-52::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:07-56-/f::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:07-56-/f::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-00::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-00::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-06::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-06::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-07::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-07::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-09-/e::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-09-/e::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-50::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-50::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-51::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-52::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-70::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-70::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-80-/a::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1/_serverconductor/_deployment_manager:08-80-/a::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-50::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-52::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-56-/Vf::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-56-/Vf::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-00::-enterprise:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-00::-standard:*.***.*.*:						
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-06::-enterprise:*.***.*.*:						

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-06:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-07:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-07:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1V_serverconductor_V_deployment_manager:08-09-Ve:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-09-Ve:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-50:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-50:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V serverconductor V deployment manager:08-51:-:standard:*.~*~*~*~*
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor V_deployment_manager:08-52:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-70:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1v_serverconductor_V_deployment_manager:08-70:-:standard:*.***.*.*:
```

```
cpe:2.3:a:hitachi:jp1v_serverconductor_v_deployment_manager:08-80-Va:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor V_deployment_manager:08-80-Va:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-50:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-52:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:07-56-Vf:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1v_serverconductor_V_deployment_manager:07-56-Vf:-:standard:*.***.*.*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor V_deployment_manager:08-00:-:enterprise:*.***.*.*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-00:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-06:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-06:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-07:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-07:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1V_serverconductor_V_deployment_manager:08-09-Ve:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1V_serverconductor_V_deployment_manager:08-09-Ve:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-50:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1v_serverconductor_v_deployment_manager:08-50:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-51:-:standard:*:*:*.*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-52:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1V_serverconductor_V_deployment_manager:08-70:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-70:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:jp1V_serverconductor_V_deployment_manager:08-80-Va:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:ip1V_serverconductor_V_deployment_manager:08-80-Va:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor/_deployment_manager:01-00:*:*:*:*.*.*
```

```
cpe:2.3:a:hitachi:serverconductor/_deployment_manager:01-01:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:hitachi:serverconductor / deployment manager:06-00:*:*:*:*.*.*
```

```
cpe:2.3:a:hitachi:serverconductor/_deployment_manager:06-00-/a:~::~~::~~::~~:::
```

```
cpe:2.3:a:hitachi:serverconductor/_deployment_manager:07-50:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor/_deployment_manager:07-50:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor / deployment_manager:07-55:-:enterprise:*.*.*.*.:
```

```
cpe:2.3:a:hitachi:serverconductor / deployment manager:07-55:-:standard:.*:.*:.*:.*
```

```
cpe:2.3:a:hitachi:serverconductor / deployment manager:07-57:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor / deployment_manager:07-57:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor / _deployment_manager:07-59:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor / deployment manager:07-59:-:standard:*:*:*.*
```

```
cpe:2.3:a:hitachi:serverconductor_v_deployment_manager:01-00:*:*:*:*.*.*
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:01-01:*****:*****:
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:06-00:***:***:***:
```

```
cpe:2.3:a:hitachi:serverconductor V deployment manager:06-00-Va:*****:*****
```

```
cpe:2.3:a:hitachi:serverconductor V deployment manager:07-50:-:enterprise:*:*:*.*.*
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-50:-:standard:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-55:-:enterprise:*.***.*.*:
```

```
cpe:2.3:a:hitachi:serverconductor_v_deployment_manager:07-55:-:standard:.*:.*:.*:.*
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-57:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-57:-:standard:*.***.*.*:
```

```
cpe:2.3:a:hitachi:serverconductor V deployment manager:07-59:-:enterprise:*:*:*:*:
```

```
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-59:-:standard:*:*:*:*:
```

cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:01-00:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:01-01:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:06-00:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:06-00-Va:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-50:-:enterprise:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-50:-:standard:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-55:-:enterprise:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-55:-:standard:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-57:-:enterprise:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-57:-:standard:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-59:-:enterprise:*****:*
cpe:2.3:a:hitachi:serverconductor_V_deployment_manager:07-59:-:standard:*****:*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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