



CVE-2012-4703

Published on: 03/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:15 PM UTC

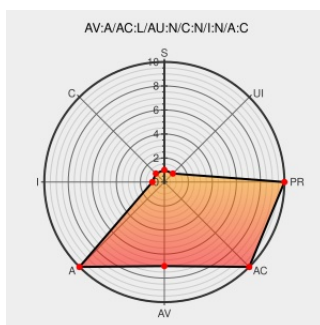
CVE-2012-4703

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Deltav Se3006 Sd Plus Controller](#) from [Emerson](#) contain the following vulnerability:

The Emerson DeltaV SE3006 through 11.3.1, DeltaV VE3005 through 10.3.1 and 11.x through 11.3.1, and DeltaV VE3006 through 10.3.1 and 11.x through 11.3.1 allow remote attackers to cause a denial of service (device restart) via a crafted packet on (1) TCP port 23, (2) UDP port 161, or (3) TCP port 513.

CVE-2012-4703 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: **6.1 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Emerson DeltaV Uncontroller Resource Consumption Vulnerability | ICS-CERT

web.archive.org

[text/html](#)

Inactive Link Not Archived

[MISC ics-cert.us-cert.gov/pdf/ICSA-13-053-01.pdf](https://ics-cert.us-cert.gov/pdf/ICSA-13-053-01.pdf)

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.

Related QID Numbers

[590586](#) Emerson DeltaV Uncontroller Resource Consumption Denial of Service (DoS) Vulnerability (ICSA-13-053-01)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emerson	Deltav Se3006 Sd Plus Controller	All	All	All	All
Application	Emerson	Deltav Ve3005 Controller Md	All	All	All	All
Application	Emerson	Deltav Ve3005 Controller Md	All	All	All	All
Application	Emerson	Deltav Ve3006 Controller Md Plus	All	All	All	All
Application	Emerson	Deltav Ve3006 Controller Md Plus	All	All	All	All

```
cpe:2.3:a:emerson:deltav_se3006_sd_plus_controller:*:*:*:*:*:
```

```
cpe:2.3:a:emerson:deltav_ve3005_controller_md:*.***.***.***:
```

```
cpe:2.3:a:emerson:deltav_ve3005_controller_md:*:*:*:*:*:
```

```
cpe:2.3:a:emerson:deltav_ve3006_controller_md_plus:*.***.***.***:
```

```
cpe:2.3:a:emerson:deltav_ve3006_controller_md_plus:*:*:*:*:*:
```

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