



CVE-2016-0281

Published on: 08/07/2016 12:00:00 AM UTC

Last Modified on: 08/31/2021 03:44:00 PM UTC

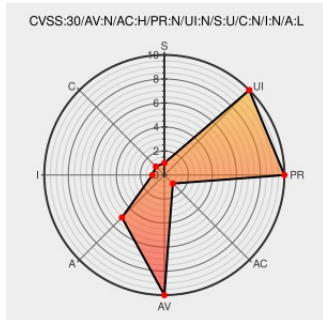
CVE-2016-0281

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Aix](#) from [Ibm](#) contain the following vulnerability:

The mustendd driver in IBM AIX 5.3, 6.1, 7.1, and 7.2 and VIOS 2.2.x, when the jumbo_frames feature is not enabled, allows remote attackers to cause a denial of service (FC1763 or FC5899 adapter crash) via crafted packets.

CVE-2016-0281 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as **LOW** severity.

CVSS3 Score: **3.7 - LOW**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
IBM notice: The page you requested cannot be displayed	Broken Link www-01.ibm.com text/html Inactive Link Not Archived	AIXAPAR IV84184

IV81459: MUSENTDD'S RECEIVE PATH HANGS WHEN IT RECEIVES CERTAIN SIZE PKT APPLIES TO AIX 7100-04	Broken Link www-01.ibm.com text/html	 AIXAPAR IV81459
IV80569: MUSENTDD'S RECEIVE PATH HANGS WHEN IT RECEIVES CERTAIN SIZE PKT APPLIES TO AIX 6100-09	Broken Link www-01.ibm.com text/html	 AIXAPAR IV80569
IBM AIX mustendd Device Driver Bug Lets Remote Users Cause the Target Adapter to Crash - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1036481
IV81357: MUSENTDD'S RECEIVE PATH HANGS WHEN IT RECEIVES CERTAIN SIZE PKT APPLIES TO AIX 7200-00	Broken Link www-01.ibm.com text/html	 AIXAPAR IV81357
	Vendor Advisory aix.software.ibm.com text/plain	 CONFIRM aix.software.ibm.com/aix/efixes/security/mustendd_advisory.asc
IBM AIX CVE-2016-0281 Remote Denial of Service Vulnerability	cve.report (archive) text/html	 BID 92193
IV82421: MUSENTDD'S RECEIVE PATH HANGS WHEN IT RECEIVES CERTAIN SIZE PKT APPLIES TO AIX 7100-03	Broken Link www-01.ibm.com text/html	 AIXAPAR IV82421

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
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	7.1	All	All	All
Operating System	Ibm	Aix	7.2	All	All	All
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	7.1	All	All	All
Operating System	Ibm	Aix	7.2	All	All	All
Application	Ibm	Vios	2.2.0.10	All	All	All
Application	Ibm	Vios	2.2.0.11	All	All	All

Application	IBM	Vios	2.2.0.11	All	All	All
Application	IBM	Vios	2.2.0.12	All	All	All
Application	IBM	Vios	2.2.0.13	All	All	All
Application	IBM	Vios	2.2.1.0	All	All	All
Application	IBM	Vios	2.2.1.1	All	All	All
Application	IBM	Vios	2.2.1.3	All	All	All
Application	IBM	Vios	2.2.1.4	All	All	All
Application	IBM	Vios	2.2.1.5	All	All	All
Application	IBM	Vios	2.2.1.6	All	All	All
Application	IBM	Vios	2.2.1.7	All	All	All
Application	IBM	Vios	2.2.1.8	All	All	All
Application	IBM	Vios	2.2.1.9	All	All	All
Application	IBM	Vios	2.2.2.0	All	All	All
Application	IBM	Vios	2.2.2.1	All	All	All
Application	IBM	Vios	2.2.2.2	All	All	All
Application	IBM	Vios	2.2.2.3	All	All	All
Application	IBM	Vios	2.2.2.4	All	All	All
Application	IBM	Vios	2.2.2.5	All	All	All
Application	IBM	Vios	2.2.3.0	All	All	All
Application	IBM	Vios	2.2.3.1	All	All	All
Application	IBM	Vios	2.2.3.2	All	All	All
Application	IBM	Vios	2.2.3.3	All	All	All
Application	IBM	Vios	2.2.3.4	All	All	All
Operating System	IBM	Vios	2.2.0.10	All	All	All
Operating System	IBM	Vios	2.2.0.11	All	All	All
Operating System	IBM	Vios	2.2.0.12	All	All	All
Operating System	IBM	Vios	2.2.0.13	All	All	All
Operating System	IBM	Vios	2.2.1.0	All	All	All
Operating System	IBM	Vios	2.2.1.1	All	All	All
Operating System	IBM	Vios	2.2.1.3	All	All	All
Operating System	IBM	Vios	2.2.1.4	All	All	All
Operating System	IBM	Vios	2.2.1.5	All	All	All

Operating System	IBM	Vios	2.2.1.5	All	All	All
Operating System	IBM	Vios	2.2.1.6	All	All	All
Operating System	IBM	Vios	2.2.1.7	All	All	All
Operating System	IBM	Vios	2.2.1.8	All	All	All
Operating System	IBM	Vios	2.2.1.9	All	All	All
Operating System	IBM	Vios	2.2.2.0	All	All	All
Operating System	IBM	Vios	2.2.2.1	All	All	All
Operating System	IBM	Vios	2.2.2.2	All	All	All
Operating System	IBM	Vios	2.2.2.3	All	All	All
Operating System	IBM	Vios	2.2.2.4	All	All	All
Operating System	IBM	Vios	2.2.2.5	All	All	All
Operating System	IBM	Vios	2.2.3.0	All	All	All
Operating System	IBM	Vios	2.2.3.1	All	All	All
Operating System	IBM	Vios	2.2.3.2	All	All	All
Operating System	IBM	Vios	2.2.3.3	All	All	All
Operating System	IBM	Vios	2.2.3.4	All	All	All
Application	IBM	Vios	2.2.0.10	All	All	All
Application	IBM	Vios	2.2.0.11	All	All	All
Application	IBM	Vios	2.2.0.12	All	All	All
Application	IBM	Vios	2.2.0.13	All	All	All
Application	IBM	Vios	2.2.1.0	All	All	All
Application	IBM	Vios	2.2.1.1	All	All	All
Application	IBM	Vios	2.2.1.3	All	All	All
Operating System	IBM	Vios	2.2.0.10	All	All	All
Operating System	IBM	Vios	2.2.0.11	All	All	All
Operating System	IBM	Vios	2.2.0.12	All	All	All

cpe:2.3:o:ibm:aix:7.1:*****:
cpe:2.3:o:ibm:aix:7.2:*****:
cpe:2.3:o:ibm:aix:5.3:*****:
cpe:2.3:o:ibm:aix:6.1:*****:
cpe:2.3:o:ibm:aix:7.1:*****:
cpe:2.3:o:ibm:aix:7.2:*****:
cpe:2.3:a:ibm:vios:2.2.0.10:*****:
cpe:2.3:a:ibm:vios:2.2.0.11:*****:
cpe:2.3:a:ibm:vios:2.2.0.12:*****:
cpe:2.3:a:ibm:vios:2.2.0.13:*****:
cpe:2.3:a:ibm:vios:2.2.1.0:*****:
cpe:2.3:a:ibm:vios:2.2.1.1:*****:
cpe:2.3:a:ibm:vios:2.2.1.3:*****:
cpe:2.3:a:ibm:vios:2.2.1.4:*****:
cpe:2.3:a:ibm:vios:2.2.1.5:*****:
cpe:2.3:a:ibm:vios:2.2.1.6:*****:
cpe:2.3:a:ibm:vios:2.2.1.7:*****:
cpe:2.3:a:ibm:vios:2.2.1.8:*****:
cpe:2.3:a:ibm:vios:2.2.1.9:*****:
cpe:2.3:a:ibm:vios:2.2.2.0:*****:
cpe:2.3:a:ibm:vios:2.2.2.1:*****:
cpe:2.3:a:ibm:vios:2.2.2.2:*****:
cpe:2.3:a:ibm:vios:2.2.2.3:*****:
cpe:2.3:a:ibm:vios:2.2.2.4:*****:
cpe:2.3:a:ibm:vios:2.2.2.5:*****:
cpe:2.3:a:ibm:vios:2.2.3.0:*****:
cpe:2.3:a:ibm:vios:2.2.3.1:*****:
cpe:2.3:a:ibm:vios:2.2.3.2:*****:
cpe:2.3:a:ibm:vios:2.2.3.3:*****:

cpe:2.3:a:ibm:vios:2.2.3.3:*****:
cpe:2.3:a:ibm:vios:2.2.3.4:*****:
cpe:2.3:o:ibm:vios:2.2.0.10:*****:
cpe:2.3:o:ibm:vios:2.2.0.11:*****:
cpe:2.3:o:ibm:vios:2.2.0.12:*****:
cpe:2.3:o:ibm:vios:2.2.0.13:*****:
cpe:2.3:o:ibm:vios:2.2.1.0:*****:
cpe:2.3:o:ibm:vios:2.2.1.1:*****:
cpe:2.3:o:ibm:vios:2.2.1.3:*****:
cpe:2.3:o:ibm:vios:2.2.1.4:*****:
cpe:2.3:o:ibm:vios:2.2.1.5:*****:
cpe:2.3:o:ibm:vios:2.2.1.6:*****:
cpe:2.3:o:ibm:vios:2.2.1.7:*****:
cpe:2.3:o:ibm:vios:2.2.1.8:*****:
cpe:2.3:o:ibm:vios:2.2.1.9:*****:
cpe:2.3:o:ibm:vios:2.2.2.0:*****:
cpe:2.3:o:ibm:vios:2.2.2.1:*****:
cpe:2.3:o:ibm:vios:2.2.2.2:*****:
cpe:2.3:o:ibm:vios:2.2.2.3:*****:
cpe:2.3:o:ibm:vios:2.2.2.4:*****:
cpe:2.3:o:ibm:vios:2.2.2.5:*****:
cpe:2.3:o:ibm:vios:2.2.3.0:*****:
cpe:2.3:o:ibm:vios:2.2.3.1:*****:
cpe:2.3:o:ibm:vios:2.2.3.2:*****:
cpe:2.3:o:ibm:vios:2.2.3.3:*****:
cpe:2.3:o:ibm:vios:2.2.3.4:*****:
cpe:2.3:a:ibm:vios:2.2.0.10:*****:
cpe:2.3:a:ibm:vios:2.2.0.11:*****:
cpe:2.3:a:ibm:vios:2.2.0.12:*****:

cpe:2.3:a:ibm:vios:2.2.0.13:*****:
cpe:2.3:a:ibm:vios:2.2.1.0:*****:
cpe:2.3:a:ibm:vios:2.2.1.1:*****:
cpe:2.3:a:ibm:vios:2.2.1.3:*****:
cpe:2.3:o:ibm:vios:2.2.0.10:*****:
cpe:2.3:o:ibm:vios:2.2.0.11:*****:
cpe:2.3:o:ibm:vios:2.2.0.12:*****:
cpe:2.3:o:ibm:vios:2.2.0.13:*****:
cpe:2.3:o:ibm:vios:2.2.1.0:*****:
cpe:2.3:o:ibm:vios:2.2.1.1:*****:
cpe:2.3:o:ibm:vios:2.2.1.3:*****:
cpe:2.3:o:ibm:vios:2.2.1.4:*****:
cpe:2.3:o:ibm:vios:2.2.1.5:*****:
cpe:2.3:o:ibm:vios:2.2.1.6:*****:
cpe:2.3:o:ibm:vios:2.2.1.7:*****:
cpe:2.3:o:ibm:vios:2.2.1.8:*****:
cpe:2.3:o:ibm:vios:2.2.1.9:*****:
cpe:2.3:o:ibm:vios:2.2.2.0:*****:
cpe:2.3:o:ibm:vios:2.2.2.1:*****:
cpe:2.3:o:ibm:vios:2.2.2.2:*****:
cpe:2.3:o:ibm:vios:2.2.2.3:*****:
cpe:2.3:o:ibm:vios:2.2.2.4:*****:
cpe:2.3:o:ibm:vios:2.2.2.5:*****:
cpe:2.3:o:ibm:vios:2.2.3.0:*****:
cpe:2.3:o:ibm:vios:2.2.3.1:*****:
cpe:2.3:o:ibm:vios:2.2.3.2:*****:
cpe:2.3:o:ibm:vios:2.2.3.3:*****:
cpe:2.3:o:ibm:vios:2.2.3.4:*****:

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](#)