



Published on: 10/31/2016 12:00:00 AM UTC

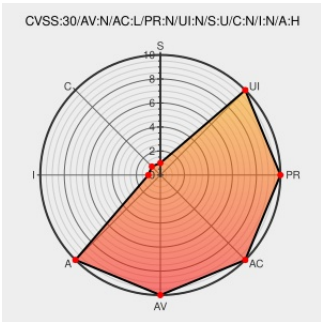
Last Modified on: 03/23/2021 11:27:09 PM UTC

CVE-2016-8203

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Netiron Os](#) from [Brocade](#) contain the following vulnerability:

A memory corruption in the IPsec code path of Brocade NetIron OS on Brocade MLXs 5.8.00 through 5.8.00e, 5.9.00 through 5.9.00bd, 6.0.00, and 6.0.00a images could allow attackers to cause a denial of service (line card reset) via certain constructed IPsec control packets.

CVE-2016-8203 has been assigned by sirt@brocade.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: 7.5 - HIGH

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

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
Support Documents and Downloads	Vendor Advisory www.brocade.com text/html	 CONFIRM www.brocade.com/en/backend-content/pdf-page.html?/content/dam/common/documents/content-types/security-bulletin/brocade-security-advisory-2016-168.pdf

Brocade NetIron OS CVE-2016-8203 Memory Corruption Vulnerability

[Third Party Advisory](#)

[🌐 BID 94232](#)

[VDB Entry](#)

[cve.report \(archive\)](#)

[text/html](#)

Brocade NetIron MLX Line Card IPSec Processing Bug Lets Remote Users Cause the Target Line Card to Reset - SecurityTracker

[www.securitytracker.com](#)

[🌐 SPECTRACK 1037010](#)

[text/html](#)

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	Brocade	Netiron Os	6.0.00	All	All	All
Operating System	Brocade	Netiron Os	6.0.00a	All	All	All
Operating System	Brocade	Netiron Os	6.0.00	All	All	All
Operating System	Brocade	Netiron Os	6.0.00a	All	All	All
Operating System	Brocade	Netiron Os	All	All	All	All
Operating System	Brocade	Netiron Os	All	All	All	All
cpe:2.3:o:brocade:netiron_os:6.0.00:*****:						
cpe:2.3:o:brocade:netiron_os:6.0.00a:*****:						
cpe:2.3:o:brocade:netiron_os:6.0.00:*****:						
cpe:2.3:o:brocade:netiron_os:6.0.00a:*****:						
cpe:2.3:o:brocade:netiron_os:*****:						
cpe:2.3:o:brocade:netiron_os:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)