



CVE-2018-18878

Published on: 06/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

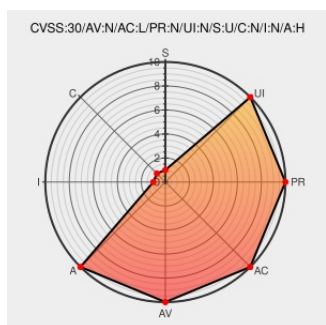
CVE-2018-18878

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Weather Microserver](#) from [Columbiaweather](#) contain the following vulnerability:

In firmware version MS_2.6.9900 of Columbia Weather MicroServer, the BACnet daemon does not properly validate input, which could allow a remote attacker to send specially crafted packets causing the device to become unavailable.

CVE-2018-18878 has been assigned by [M](#) cve@mitre.org 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
Applied Risk :: Advisories	Third Party Advisory applied-risk.com text/html	MISC applied-risk.com/labs/advisories
Columbia Weather Systems MicroServer CISA	Third Party Advisory	MISC ics-cert.us-cert.gov/advisories/ICSA-19-078-02

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Columbiaweather	Weather Microserver	-	All	All	All
Hardware 	Columbiaweather	Weather Microserver	-	All	All	All
Operating System	Columbiaweather	Weather Microserver Firmware	ms_2.6.9900	All	All	All
Operating System	Columbiaweather	Weather Microserver Firmware	ms_2.6.9900	All	All	All
<pre>cpe:2.3:h:columbiaweather:weather_microserver:-:*:*:*:*:*:</pre>						
<pre>cpe:2.3:h:columbiaweather:weather_microserver:-:*:*:*:*:*:</pre>						
<pre>cpe:2.3:o:columbiaweather:weather_microserver_firmware:ms_2.6.9900:*:*:*:*:*:</pre>						
<pre>cpe:2.3:o:columbiaweather:weather_microserver_firmware:ms_2.6.9900:*:*:*:*:*:</pre>						