



CVE-2023-2186

Published on: Not Yet Published

Last Modified on: 06/16/2023 06:05:00 PM UTC

CVE-2023-2186

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Scada Data Gateway](#) from [Trianglemicroworks](#) contain the following vulnerability:

On Triangle MicroWorks' SCADA Data Gateway version $\leq$ v5.01.03, an unauthenticated attacker can send a specially crafted broadcast message including format string characters to the SCADA Data Gateway to perform unrestricted memory reads. An unauthenticated user can use this format string vulnerability to repeatedly crash the

GTWebMonitor.exe process to DoS the Web Monitor. Furthermore, an authenticated user can leverage this vulnerability to leak memory from the GTWebMonitor.exe process. This could be leveraged in an exploit chain to gain code execution.

CVE-2023-2186 has been assigned by trellixpsirt@trellix.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Triangle MicroWorks](#) - **SCADA Data Gateway** version = **5.01.03**

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
Industrial and Manufacturing CVEs: Addressing the SCADA in the Room	www.trellix.com text/html	MISC www.trellix.com/en-us/about/newsroom/stories/research/industrial-and-manufacturing-cves.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
Application	Trianglemicroworks	Scada Data Gateway	All	All	All	All
cpe:2.3:a:trianglemicroworks:scada_data_gateway:*****:.*						

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](#)