



CVE-2021-38457

Published on: 10/22/2021 12:00:00 AM UTC

Last Modified on: 10/27/2022 04:33:00 PM UTC

CVE-2021-38457 - advisory for <https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01>

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Versiondog](#) from [Auvesy](#) contain the following vulnerability:

The server permits communication without any authentication procedure, allowing the attacker to initiate a session with the server without providing any form of authentication.

CVE-2021-38457 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [AUVESY](#) - **Versiondog** version <= 8.0

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
AUVESY Versiondog CISA	us-cert.cisa.gov text/html	CONFIRM us-cert.cisa.gov/ics/advisories/icsa-21-292-01

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

[590588](#) AUVESY Versiondog Multiple Vulnerabilities (ICSA-21-292-01)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auvesy	Versiondog	All	All	All	All
cpe:2.3:a:auvesy:versiondog:*:*:*:*:*:						

Discovery Credit

Amir Preminger of Claroty reported these vulnerabilities to CISA.

Social Mentions

Source	Title	Posted (UTC)
 @management_sun	IT Risk:AUVESY製Versiondogにおける複数の脆弱性 -1/2 CVSS v3=9.8を含む複数の脆弱性 CVE-2021-38457 CVE-2021-38475 CVE-2021-38461 CVE-2021... twitter.com/i/web/status/1...	2021-10-22 01:46:39
 @CVEreport	CVE-2021-38457 : The server permits communication without any authentication procedure, allowing the attacker to in... twitter.com/i/web/status/1...	2021-10-22 12:05:56
 @threatmeter	CVE-2021-38457 The server permits communication without any authentication procedure, allowing the attacker to init... twitter.com/i/web/status/1...	2021-10-23 07:09:52

[← 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](#)