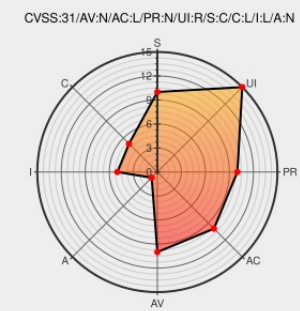
CVE-2021-33001

Published on: Not Yet Published

Last Modified on: 05/25/2022 01:52:00 PM UTC

CVE-2021-33001

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xarrow from Xarrow contain the following vulnerability:

xArrow SCADA versions 7.2 and prior is vulnerable to cross-site scripting due to parameter ‘bdate’ of the resource xhisvalue.htm, which may allow an unauthorized attacker to execute arbitrary code.

CVE-2021-33001 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **xArrow** - **xArrow SCADA** version **<= 7.2**

Vulnerability Patch/Work Around

xArrow has not responded to requests to work with CISA to mitigate these vulnerabilities. Users of these affected products who would like to see more responsible security are invited to contact xArrow customer support.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should: Disable web server implementation. Web server is disabled by default. Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Locate control system networks and remote devices behind firewalls, and isolate them from the business network. When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices. CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
xArrow SCADA | CISA	www.cisa.gov text/html	CONFIRM www.cisa.gov/uscert/ics/advisories/icsa-21-229-03

Related QID Numbers

590525 xArrow SCADA Multiple Vulnerabilities (ICSA-21-229-03)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xarrow	Xarrow	All	All	All	All

cpe:2.3:a:xarrow:xarrow:*:*:*:*:*:*:*:*:

Discovery Credit

Sharon Brizinov from Claroty, and Michael Heinzl reported these vulnerabilities to CISA.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-33001 : xArrow SCADA versions 7.2 and prior is vulnerable to cross-site scripting due to parameter 'bdate'… twitter.com/i/web/status/1…	2022-05-16 18:09:33
/r/netcve	CVE-2021-33001	2022-05-16 18:38:38

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report