Clorius Controls A/S ISC SCADA Insecure Java Client Inadequate Encryption Strength

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-9199
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-17 02:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Clorius Controls Java web client before 01.00.0009g allows remote attackers to discover credentials by sniffing the net

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-326 | CWE-200 | CWE-326 CWE-326

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N
2.0	ics-cert@hq.dhs.gov	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	CVSS	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clorius Controls A S	Java Web Client	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Clorius Controls	A/S Java Web Client	affected 01.00.0009b custom	Not specified

References

Reference	Source	Link
Clorius Controls A/S ISC SCADA Insecure Java Client Web Authentication | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-cer
www.cloriuscontrols.com	ics-cert@hq.dhs.gov	www.c
www.cisa.gov/news-events/ics-advisories/icsa-15-013-02	ics-cert@hq.dhs.gov	www.c
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

Vendor Comments And Credit

Discovery Credit

CNA: Aditya Sood (en)

Additional Advisory Data

Solutions

CNA: Clorius Controls A/S produced an update (Version 01.00.0009g) that mitigates this vulnerability. Contact Clorius Controls A/S for more information at: http://www.cloriuscontrols.com

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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