



CVE-2018-8096

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-8096
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-14 00:29:00 UTC
Updated	2019-02-28 18:07:00 UTC
Description	Datalust Seq before 4.2.605 is vulnerable to Authentication Bypass (with the attacker obtaining admin access) via ""Name":'

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Datalust	Seq	All	All	All	All
Application	Datalust	Seq	All	All	All	All

References

Reference	Source	Link
Bypass Admin Authentication on Seq - stolabs - Medium	MISC	medium.com
Seq 4.2.476 - Authentication Bypass - Windows webapps Exploit	EXPLOIT-DB	www.exploit-db.com
CVE-2018-8096 Authentication bypass in builds up to and including 4.2.476 · Issue #675 · datalust/seq-tickets · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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