



CVE-2020-25068

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

Summary

CVE	CVE-2020-25068
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-03 15:15:00 UTC
Updated	2020-11-12 22:15:00 UTC
Description	Setelsa Conacwin v3.7.1.2 is vulnerable to a local file inclusion vulnerability. This vulnerability allows a remote unauthenticated user to execute arbitrary code on the target system.

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Setelsa-security	Conacwin	3.7.1.2	All	All	All
Application	Setelsa-security	Conacwin	3.7.1.2	All	All	All

References

Reference	Source	Link	Tags
[POC] LFI Conacwin v3.7.1.2 - YouTube	MISC	www.youtube.com	Exploit, Third Party Adv
Control de acceso - Setelsa Security	MISC	setelsa-security.es	Vendor Advisory
GitHub - bryanroma/CVE-2020-25068: Python script to exploit CVE-2020-25068.	MISC	github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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