CVE-2020-8655

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

Summary

CVE	CVE-2020-8655
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-07 00:15:00 UTC
Updated	2022-01-01 19:57:00 UTC
Description	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, a

Risk And Classification

EPSS: 0.883790000 probability, percentile 0.995050000 (date 2026-05-07)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-269

CISA Known Exploited Vulnerability

Vendor	EyesOfNetwork
Product	EyesOfNetwork
Name	EyesOfNetwork Improper Privilege Management Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-8655

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eyesofnetwork	Eyesofnetwork	5.3-0	All	All	All
Application	Eyesofnetwork	Eyesofnetwork	5.3-0	All	All	All

References

Reference	Source	Link
EyesOfNetwork AutoDiscovery Target Command Execution ≈ Packet Storm	MISC	packetsto
EyesOfNetwork 5.3 Remote Code Execution ≈ Packet Storm	MISC	packetsto
Elevation de privilèges possible depuis l'utilisateur apache. · Issue #8 · EyesOfNetworkCommunity/eonconf · GitHub	MISC	github.co

CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730386 EyesOfNetwork Multiple Vulnerabilities