



CVE-2022-43441

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

Summary

CVE	CVE-2022-43441
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-16 21:15:00 UTC
Updated	2023-03-22 21:01:00 UTC
Description	A code execution vulnerability exists in the Statement Bindings functionality of Ghost Foundation node-sqlite3 5.1.1. A spec

Risk And Classification

Problem Types: CWE-913

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ghost	Sqlite3	All	All	All	All

References

Reference	Source	Link	Tags
TALOS-2022-1645 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
Code execution vulnerability due to Object coercion - Advisory · TryGhost/node-sqlite3 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181657](#) Debian Security Update for node-sqlite3 (DSA 5373-1)

[183147](#) Debian Security Update for node-sqlite3 (CVE-2022-43441)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)