IoT Advisory Board

August 2023 Meeting

Draft – For Discussion Purposes

IoT AB Cybersecurity Subgroup

Subgroup Members:

- Mike Bergman
- Ranveer Chandra
- Steve Griffith
- Tom Katsioulas
- Kevin Kornegay
- Pete Tseronis

Consumer Technology Association™

August 2023 Subgroup Update

New Draft Recommendations

Recommendation 6: Guidance to Clarify IoT Sector Boundaries

The federal government should promote and support the development of an overarching guideline developed in a multi-stakeholder process that more clearly distinguishes the major sectors of the IoT for use when dealing with concerns such as cybersecurity.

Recommendation 7: Technical Guidance on IoT Vulnerabilities

The government should consider additional ways to highlight those vulnerabilities most likely to be applicable to IoT product developers.

Draft – For Discussion Purposes

Recommendation #6 (details)

Delineate IoT Sectors

Create guidance on and promote a distinction between IoT, IIoT and Process Sensors and to address the lack of cyber security and trust in legacy process sensors and IIoT devices among multiple stakeholders.

Justification

Two large sectors in IoT are Consumer IoT and Industrial IoT. Other connected device categories exist for automotive, medical, aviation, and more. Regulators and legislators would benefit from guidance to correctly identify where one sector ends and another begins, and where the overlaps are.

Draft – For Discussion Purposes

Recommendation #7 (details)

Highlight vulnerabilities most likely to be applicable to IoT product developers.

Provide guidance to IoT developers to help them efficiently comply with standards or best practices for addressing “critical vulnerabilities” or “known vulnerabilities”.

For example, by providing a list of known IoT operating system vulnerabilities that developers should be aware of and address, or a means to filter an existing list for such vulnerabilities.

Justification

An IoT developer is encouraged or required to make sure they address any “known vulnerabilities” or “critical vulnerabilities” as part of best practices. The FCC NPRM on the U.S. Cyber Trust Mark program mentions “identified security vulnerabilities” @58 and “critical patches” @40.

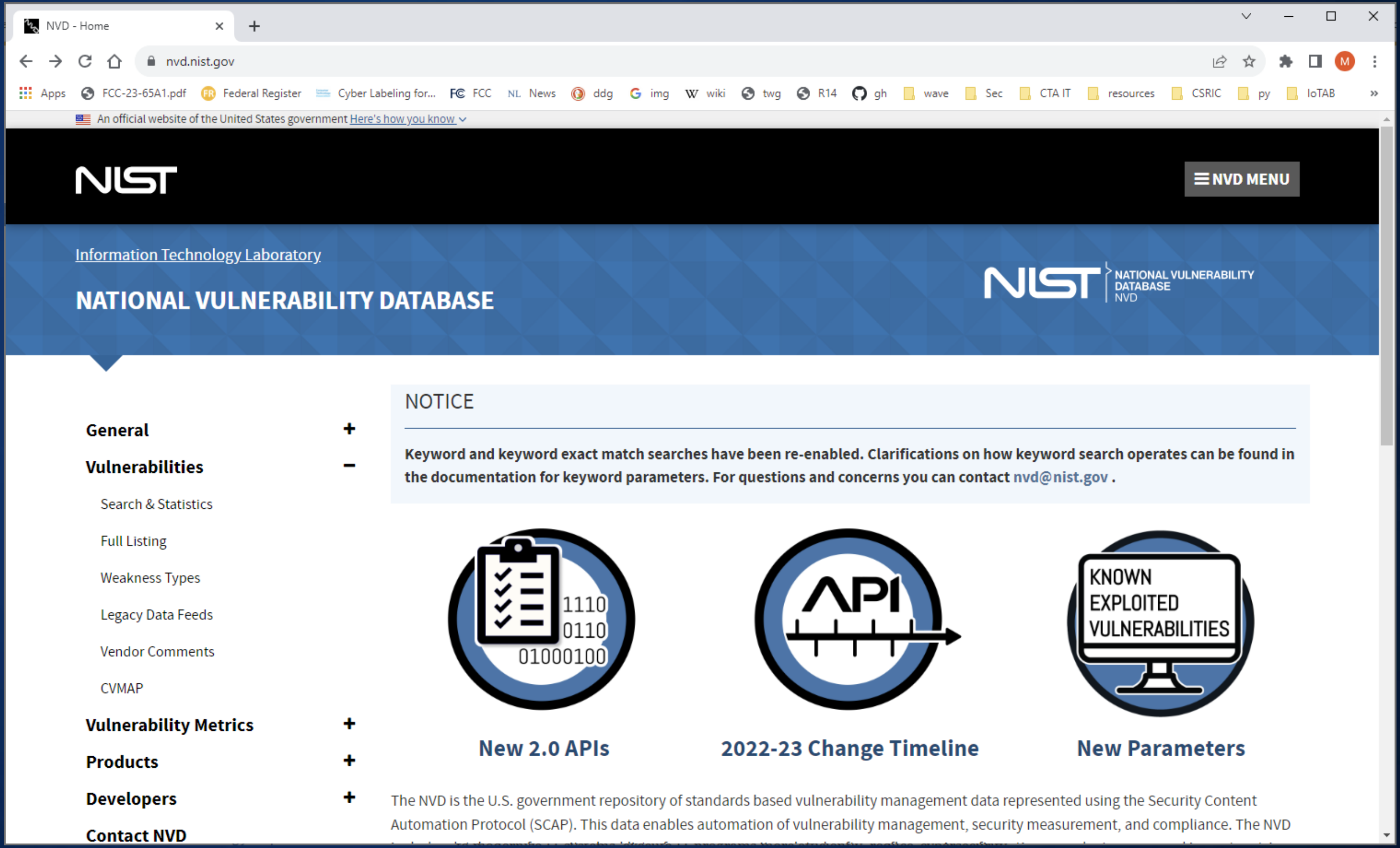
There is currently no resource that matches this “known” or “critical” criteria for IoT vulnerabilities.

Draft – For Discussion Purposes

NIST Maintains a National Vulnerability Database

https://nvd.nist.gov

(1,173 entries for keyword "IoT" !)



An official website of the United States government Here's how you know

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NOTICE

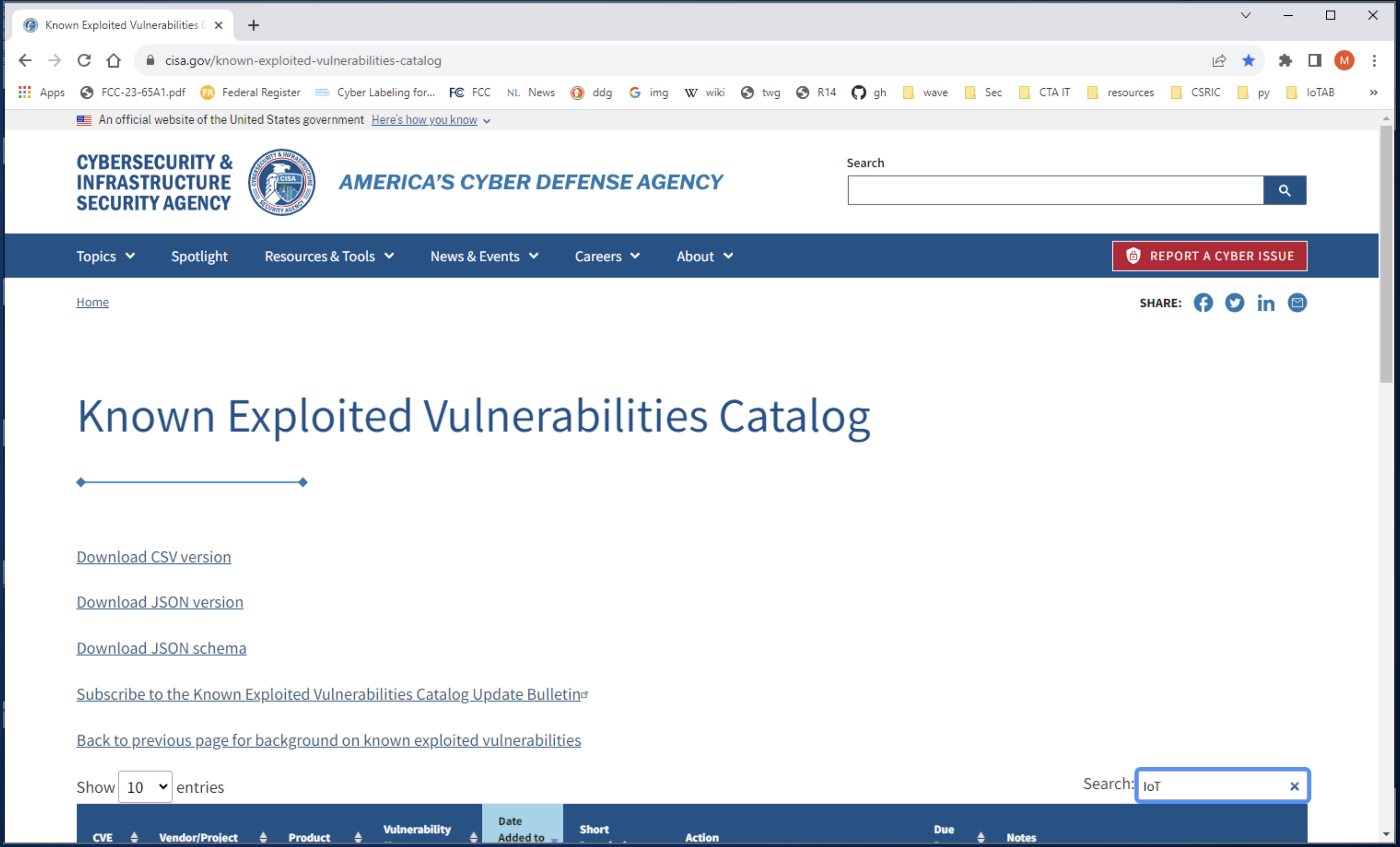
Keyword and keyword exact match searches have been re-enabled. Clarifications on how keyword search operates can be found in the documentation for keyword parameters. For questions and concerns you can contact nvd@nist.gov .

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD

CISA Maintains a Known Exploited Vulnerabilities Catalog

https://nvd.nist.gov

(1 entry for keyword "IoT" !)


Known Exploited Vulnerabilities C
cisa.gov/known-exploited-vulnerabilities-catalog
Apps
FCC-23-65A1.pdf
Federal Register
Cyber Labeling for...
FCC
News
ddg
img
wiki
twg
R14
gh
wave
Sec
CTA IT
resources
CSRIC
py
IoTAB
An official website of the United States government Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home
SHARE:

Known Exploited Vulnerabilities Catalog

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Show 10 entries

Search: IoT

CVE	Vendor/Project	Product	Vulnerability	Date Added to	Short	Action	Due	Notes

Discussion