CVE-2020-7369

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

Summary

CVE	CVE-2020-7369
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-20 17:15:00 UTC
Updated	2020-10-21 13:33:00 UTC
Description	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of the Yandex Browser allows a

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yandex	Yandex Browser	All	All	All	All
Application	Yandex	Yandex Browser	All	All	All	All

References

Reference	Source	Link
[Vuln Disclosure] Mobile Browser Bar Spoofing Vulnerabilities	MISC	blog.rapid7.c
Multiple Address Bar Spoofing Vulnerabilities In Mobile Browsers - Miscellaneous Ramblings of A Ethical Hacker	MISC	www.rafaybal
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Rafay Baloch, and disclosed in accordance with Rapid7's coordinated vulnerability disclosure policy at https://www.rapid7.com/security/disclosure#zeroday

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