CVE-2016-8503

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

Summary

CVE	CVE-2016-8503
State	PUBLISHED
Assigner	yandex
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-26 18:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Yandex Protect Anti-phishing warning in Yandex Browser for desktop from version 16.7 to 16.9 could be used by remote att

Risk And Classification

Primary CVSS: v3.0 7.3 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

EPSS: 0.001940000 probability, percentile 0.410540000 (date 2026-05-09)

Problem Types: CWE-254 | Password brute-force through Yandex Protect Anti-phishing message

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yandex	Yandex Browser	16.7.0.3342	All	All	All
Application	Yandex	Yandex Browser	16.7.1.20808	All	All	All
Application	Yandex	Yandex Browser	16.9.1.1131	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yandex N.V.	Yandex Browser For Desktop	affected 16.7 to 16.9 for Windows and OSx.	Not specified

References

Reference	Source	Link
Vulnerability fix history for Yandex Browser	af854a3a-2127-422b-91ae-364da2661108	browser.yan
Yandex Browser CVE-2016-8503 Brute Force Authentication Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securit
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**