



CVE-2019-16917

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

Summary

CVE	CVE-2019-16917
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-17 18:15:00 UTC
Updated	2019-10-22 18:35:00 UTC
Description	WiKID Enterprise 2FA (two factor authentication) Enterprise Server through 4.2.0-b2047 is vulnerable to SQL injection through the 'id' parameter in the 'login' endpoint. An attacker can exploit this vulnerability to gain access to the system. (CWE-89)

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wikidsystems	Two Factor Authentication Enterprise Server	All	All	All	All

References

Reference	Source	Link
Full Disclosure: WiKID 2FA Enterprise Server Multiple Issues	FULLDISC	seclists.org
WiKID Systems 2FA Enterprise Server 4.2.0-b2032 SQL Injection / XSS / CSRF ≈ Packet Storm	MISC	packetstormsecurity.com
WiKID Systems 2FA Enterprise Server SQL injection	MISC	www.securitymetrics.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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