



CVE-2020-11579

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

Summary

CVE	CVE-2020-11579
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-03 18:15:00 UTC
Updated	2023-02-03 19:01:00 UTC
Description	An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation pro

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chadhaajay	Phpkb	9.0	All	All	All
Application	Chadhaajay	Phpkb	9.0	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All

References

Reference
GitHub - ShielderSec/CVE-2020-11579: Exploit code for CVE-2020-11579, an arbitrary file disclosure through the MySQL client in PHPKB
The Leader in Knowledge Base Software PHPKB
Knowledge Management Software, Knowledge Base Software PHPKB
Sometimes they come back: exfiltration through MySQL and CVE-2020-11579 - Shielder
Shielder - Web Security & Design
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)