Unauthenticated SQL Injection via Search engine

High **trasher** published **GHSA-346p-qj3v-9rxj** 2 weeks ago

Package

glpi (glpi)

Affected versions

>= 11.0.0

Patched versions

11.0.6

Description

Impact

An unauthenticated time-based blind SQL injection exists in GLPI's Search engine.

Patches

Upgrade to 11.0.6.

Workaround

Disable anonymous access to the FAQ so that this security vulnerability can only be exploited by an authenticated user.

For more information

If you have any questions or comments about this advisory, mail us at glpi-security@ow2.org.

Severity

High 8.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-26263

Weaknesses

▶ CWE-89

Credits

BZHunt	Reporter
aarjubh	Reporter