



CVE-2023-3310

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

Summary

CVE	CVE-2023-3310
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-18 12:15:00 UTC
Updated	2023-11-07 04:18:00 UTC
Description	A vulnerability, which was classified as critical, has been found in code-projects Agro-School Management System 1.0. Affected versions are 1.0.0 through 1.0.1. The vulnerability allows a remote attacker to execute arbitrary code on the target system. The vulnerability is due to a buffer overflow in the loaddata.php script. The attacker can exploit this by sending a specially crafted request to the loaddata.php script. This results in a denial of service (DoS) condition. The vulnerability is present in the code-projects Agro-School Management System 1.0.0 through 1.0.1. The vulnerability is classified as critical because it allows a remote attacker to execute arbitrary code on the target system. The vulnerability is due to a buffer overflow in the loaddata.php script. The attacker can exploit this by sending a specially crafted request to the loaddata.php script. This results in a denial of service (DoS) condition. The vulnerability is present in the code-projects Agro-School Management System 1.0.0 through 1.0.1. The vulnerability is classified as critical because it allows a remote attacker to execute arbitrary code on the target system.

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Agro-school Management System Project	Agro-school Management System	1.0	All	All	All

References

Reference	Source	Link
Login required	MISC	vuldb.com
CVE-2023-3310: code-projects Agro-School Management System loaddata.php sql injection	MISC	vuldb.com
CVEHub/Agro-School Management System loaddata.php has Sqlinjection.pdf at main · humaowei/CVEHub · GitHub	MISC	github.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