Vulnerabilities overview.

In April, 2023, 2 vulnerabilities had been publicly released.

CVE-2023-2055.

The vulnerability has been publicly released on April 15, 2023. Its description is:

A vulnerability has been found in Campcodes Advanced Online Voting System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/config_save.php. The manipulation of the argument title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225940.

Its CVSS score is not provided.

Associated reports.

No entities found.

Recommendations.

No entities found.

CVE-2023-2044.

It has been publicly released on April 15, 2023. The vulnerability's description is:

A vulnerability has been found in Control iD iDSecure 4.7.29.1 and classified as problematic. This vulnerability affects unknown code of the component Dispositivos Page. The manipulation of the argument IP-DNS leads to cross site scripting. The attack can be initiated remotely. VDB-225922 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Its CVSS score is not provided.

Associated reports.

No entities found.

Recommendations.

No entities found.