Impactful vulnerabilities detected S0106-cmd [CVE-2023-2055,CVE-2023-2044]

Overview

S0106-cmd is vulnerable to ...
An attacker can use it to ...

The CTI team at Leonardo has detected the following vulnerabilities CVE-2023-2055 and CVE-2023-2044.

Description

S0106-cmd is a tool. The description of S0106-cmd is: [cmd] is the Windows command-line interpreter that can be used to interact with systems and execute other processes and utilities.

Cmd.exe contains native functionality to perform many operations to interact with the system, including listing files in a directory (e.g., dir), deleting files (e.g., del), and copying files (e.g., copy).

On 15 April 2023, 2 vulnerabilities have been disclosed.

Cve-2023-2055 is a vulnerability. The description of the vulnerability 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. It cvss score is 7.0. The security flaw exploitability score is 7.0. Cve-2023-2055 impact score is 5.9. Cve-2023-2055 is present in products offered by MaskOff. The security flaw affects these products Tolly and Xeria.

Cve-2023-2044 is a vulnerability. The description of the security flaw 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. The security flaw cvss score is 6.0. Cve-2023-2044 exploitability score is 4.0. It impact score is 4.0. The security flaw is present in products offered by ChipMasters. Cve-2023-2044 affects this product Volley.

The table below includes further details about the vulnerabilities, including the product affected by the security flaw, vendor, CVSSv2 and CVSSv3 score.

ID	CVSSv2	CVSSv3	Vendor	Products	Name
CVE-2023-2055	7.0	6.9	MaskOff	Tolly and Xeria	CVE-2023-2055
CVE-2023-2044	6.0	5.9	ChipMasters	Volley	CVE-2023-2044

Mitigations

Recommended Actions

In line with the CISA guidelines, and following the instructions of the relevant vendor, it is advisable, where possible, to install the latest security updates for products affected by the above vulnerabilities. It is also advisable to prioritize the patching of vulnerabilities affecting services exposed on the Internet and then those with higher CVSS scores.

Appendix 1

CVE-2023-2055 CVSS 3.0: 6.9
Vulnerability Description: 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.
Recommended Mitigations: Human User Authentication and Communication Authenticity
Detection Methods: List of detection methods
Vulnerable Configurations: None

CVSS3					
Base	6.9	Impact	5.9	Exploitability	6.7
Access	Attack Complexity	Attack vector	Privileges Required	Scope	User Interaction
	Low	Local	Low	unchanged	Required
Impact	Confidentiality		Integrity	Availability	
	Low		Low	High	

Source

None

Appendix 2

CVE-2023-2044 CVSS 3.0: 5.9
Vulnerability Description: 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.
Recommended Mitigations: Data Transfer Size Limits Mitigation
Detection Methods: List of detection methods
Vulnerable Configurations: Version 2.0.1 and later

CVSS3					
Base	5.9	Impact	3.9	Exploitability	3.9
Access	Attack Complexity	Attack vector	Privileges Required	Scope	User Interaction
	High	Network	High	unchanged	None
Impact	Confidentiality		Integrity	Availability	
	Low		None	None	

Source

None