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 powerful tool that serves as the Windows command-line interpreter. Its main purpose is to enable users to interact with systems and execute various processes and utilities. Its native functionality allows for seamless operations, including the ability to list files in a directory using "dir," delete files using "del," and copy files using "copy."

On 15 April 2023, 2 vulnerabilities have been disclosed.

Cve-2023-2055 is a troublesome vulnerability that has been discovered in Campcodes Advanced Online Voting System 1.0. The vulnerability pertains to an unknown code within the file /admin/config_save.php. When the argument 'title' is manipulated, it can lead to cross site scripting, which can be initiated remotely. Furthermore, the exploit has been made public and could potentially be utilized by hackers. The vulnerability, identified as VDB-225940, has a cvss score of 7.0, with an equal security flaw exploitability score. Cve-2023-2055 has an impact score of 5.9 and is present in products offered by MaskOff, including Tolly and Xeria.

Cve-2023-2044 is a problematic vulnerability found in Control iD iDSecure 4.7.29.1. The vulnerability affects the Dispositivos Page component and can lead to cross-site scripting by manipulating the IP-DNS argument. Attackers can initiate this remotely. The vulnerability has been assigned identifier VDB-225922 and has a security flaw CVSS score of 6.0, exploitability score of 4.0, and impact score of 4.0. The vulnerability affects ChipMasters' Volley product, but despite early disclosure, the vendor did not respond in any way.

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-	7.0	6.9	MaskOff	Tolly and	CVE-2023-

2055				Xeria	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