Carlo Gavazzi EOS Box Hard-Coded Credentials

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-6428
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-23 21:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The Carlo Gavazzi EOS-Box stores hard-coded passwords in the PHP file of the device. By using the hard-coded passwor

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-798 | CWE-255 | CWE-798 CWE-798

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	ics-cert@hq.dhs.gov	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	CVSS	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Carlosgavazzi	Eos-box Photovoltaic Monitoring System	-	All	All	All
Operating System	Carlosgavazzi	Eos-box Photovoltaic Monitoring System Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Carlo Gavazzi Automation	EOS-Box	affected 1.0.0.1080_2.1.10 custom	Not specified

References

Reference	Source	Link	Tags
Carlo Gavazzi EOS Box Multiple Vulnerabilities | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	www.us-cert.gov	US Governme
www.cisa.gov/news-events/ics-advisories/icsa-12-354-02	ics-cert@hq.dhs.gov	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Carlo Gavazzi has developed a new firmware Version 1.0.0.1080_2.1.10 that mitigates these vulnerabilities. Carlo Gavazzi released the new firmware Tuesday, December 18, 2012, directly to the devices. Users will be able to manually download the firmware on their device by using the Firmware Update function in the System Menu in the device's Web interface.

There are currently no legacy QID mappings associated with this CVE.