



CVE-2021-38485

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

Summary

CVE	CVE-2021-38485
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-22 14:15:00 UTC
Updated	2021-10-27 15:23:00 UTC
Description	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Emerson	Wireless 1410d Gateway	All	All	All	All
Operating System	Emerson	Wireless 1410d Gateway Firmware	All	All	All	All
Hardware	Emerson	Wireless 1410 Gateway	All	All	All	All
Operating System	Emerson	Wireless 1410 Gateway Firmware	All	All	All	All
Hardware	Emerson	Wireless 1420 Gateway	-	All	All	All
Operating System	Emerson	Wireless 1420 Gateway Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Emerson WirelessHART Gateway CISA	CONFIRM	us-cert.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Amir Preminger of Claroty reported these vulnerabilities to CISA

591140 Emerson WirelessHART Gateway Multiple Vulnerabilities (ICSA-21-278-02)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)