

Forum:[Hack Forums](#)

Thread: [Gralp Systems Gralp FMUS series](#)

Stanley - August 14, 2025, 4:20 am

Güralp Systems Güralp FMUS series

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 9.3

ATTENTION: Exploitable remotely/Low attack complexity

Vendor: Güralp Systems

Equipment: Güralp FMUS Series Seismic Monitoring Devices

Vulnerability: Missing Authentication for Critical Function

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to modify hardware configurations, manipulate data, or factory reset the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Güralp FMUS series are affected:

Güralp FMUS Series Seismic Monitoring Devices: All versions

3.2 Vulnerability Overview

3.2.1 MISSING AUTHENTICATION FOR CRITICAL FUNCTION CWE-306

The affected products expose an unauthenticated Telnet-based command line interface that could allow an attacker to modify hardware configurations, manipulate data, or factory reset the device.

CVE-2025-8286 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2025-8286. A base score of 9.3 has been calculated; the CVSS vector string is

(AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: United Kingdom

3.4 RESEARCHER

Souvik Kandar of MicroSec (microsec.io) reported this vulnerability to CISA.

4. MITIGATIONS

Güralp did not respond to CISA's attempts at coordination. Users of Güralp are encouraged to contact Güralp and keep their systems up to date.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov/ics](https://www.cisa.gov/ics). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov/ics](https://www.cisa.gov/ics) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

5. UPDATE HISTORY

July 31, 2025: Initial Publication

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-212-01>

JoseMar - September 3, 2025, 1:46 pm

The vendor didn't even respond is honestly the most shocking part.????