

Forum:[Hack Forums](#)

Thread: [Güralp Systems Fortimus Series, Minimus Series, and Certimus Series](#)

Stanley - January 8, 2026, 7:05 am

Güralp Systems Fortimus Series, Minimus Series, and Certimus Series

View CSAF

Summary

Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service condition.

The following versions of Güralp Systems Fortimus Series, Minimus Series, and Certimus Series are affected:

Fortimus Series (CVE-2025-14466)

Minimus Series (CVE-2025-14466)

Certimus Series (CVE-2025-14466)

CVSS

Vendor

Equipment

Vulnerabilities

v3 5.3

Güralp Systems

Güralp Systems Fortimus Series, Minimus Series, and Certimus Series

Allocation of Resources Without Limits or Throttling

Background

Critical Infrastructure Sectors: Critical Manufacturing

Countries/Areas Deployed: Worldwide

Company Headquarters Location: United Kingdom

Vulnerabilities

Expand All +

CVE-2025-14466

A vulnerability in the web interface of the Güralp Fortimus Series, Minimus Series and Certimus Series allows an unauthenticated attacker with network access to send specially-crafted HTTP requests that can cause the web service process to deliberately restart. Although this mechanism limits the impact of the attack, it results in a brief denial-of-service condition during the restart.

[View CVE Details](#)

Affected Products

Güralp Systems Fortimus Series, Minimus Series, and Certimus Series

Vendor:Güralp Systems

Product Version:Güralp Systems Fortimus Series: vers:all/*, Güralp Systems Minimus Series: vers:all/*, Güralp Systems Certimus Series: vers:all/*

Product Status:known_affected

Remediations

MitigationGüralp Systems recommends that users operate their systems behind a NAT or VPN firewall. For more information, please contact Güralp Systems.

Relevant CWE: CWE-770 Allocation of Resources Without Limits or Throttling

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.1

5.3

MEDIUM

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Acknowledgments

Souvik Kandar reported this vulnerability to CISA.

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

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.

Revision History

Initial Release Date: 2025-12-16

Date

Revision

Summary

2025-12-16

1

Initial Publication

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-350-01>