THREAT BULLETINS

Critical CrushFTP Flaw Actively Exploited, PoC Exploit Code Available

TLP:WHITE

Apr 01, 2025

A critical vulnerability, tracked as CVE-2025-2825, affecting CrushFTP is actively being exploited following the release of proof-of-concept exploit code.

The vulnerability is an authentication bypass flaw that allows remote threat actors to gain unauthenticated access to infrastructure running unpatched CrushFTP v10 or v11 software exposed on the Internet over HTTP(S).

According to the monitoring platform Shadowserver, targeted exploitation attempts against CrushFTP were observed approximately a week after the vulnerability was disclosed.

The discovery by Shadowserver, in which over 1,500 flawed instances were exposed online, highlights the speed at which threat actors begin attempted exploitation attacks against vulnerable products or services. This is evident in how quickly the vulnerability was targeted after a write-up containing technical details about CVE-2025-2825 and proof-of-concept exploit code was released.

Health-ISAC provides this information for situational awareness and encourages users to upgrade affected CrushFTP versions

immediately, as threat actors have exhibited high interest in exploiting vulnerable file transfer products.

Recommendations:

- Apply available patches for vulnerable CrushFTP instances.
- Enable DMZ (demilitarized zone) perimeter network option if updating is not feasible
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	Bleeping Computer, , Help Net Security, X.Org, crushftp

Alert ID 8db083cc

View Alert

Share Feedback

was this helpful?  | 

Tags CVE-2025-2825, CrushFTP

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.