

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware CrushFTP published a security advisory to address a vulnerability in the following product:

- CrushFTP – versions prior to 10.7.1 and 11.x versions prior to 11.1.0

Technical Details

CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a [DMZ](#) in front of their main CrushFTP instance are partially protected with its protocol translation system it utilizes. A DMZ however does not fully protect you and you must update immediately. (CREDIT:Simon Garrelou, of Airbus CERT)

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify [VRM](#) with any questions or concerns you may have.

References

- [CVE-2024-4040](#)
- [CrushFTP Update](#)