Security Advisory 2024-061

Vulnerabilities in Nextcloud Products

June 18, 2024 — v1.0

TLP:CLEAR

History:
- 18/06/2024 — v1.0 – Initial publication

Summary

On June 14, 2024, Nextcloud released patches for Nextcloud Server and Enterprise Server. A vulnerability was disclosed in Nextcloud server products that allows the bypassing of the second factor of two-factor authentication (2FA) [1,2].

Technical Details

The vulnerability CVE-2024-37313, with a CVSS score of 7.3, is a 2FA bypass issue. Under certain circumstances, an attacker could exploit this vulnerability to bypass the second factor of 2FA after successfully providing the user credentials [1].

Affected Products

Patched versions of the products are listed below [1,3].
- Nextcloud Server: Versions 26.0.13, 27.1.8 and 28.0.4.

Recommendations

CERT-EU strongly recommends updating affected software to the latest versions by following the instructions given by the vendor [1].

References

[1] https://github.com/nextcloud/security-advisories/security/advisories/GHSA-9v72-9xv5-3p7c