SMTP Command Injection in iCalendar Attachments to emails via newlines

Moderate **nickvergessen** published **GHSA-264h-3v4w-6xh2** on Jul 4

Package

Server (Nextcloud)

Affected versions	Patched versions
< 22.2.8, < 23.0.5, < 24.0.1	22.2.8, 23.0.5, 24.0.1

Server (Nextcloud Enterprise)

<19.0.13.7, <20.0.14.6, <21.0.9.5, <22.2.8, <23.0.5	19.0.13.7, 20.0.14.6, 21.0.9.5, 22.2.8, 23.0.5

Description

Impact

The impact varies based on which commands are supported by the backend SMTP server. However, the main risk here is that the attacker can then hijack an already-authenticated SMTP session and run arbitrary SMTP commands as the email user, such as sending emails to other users, changing the FROM user, and so on. As before, this depends on the configuration of the server itself, but newlines should be sanitized to mitigate such arbitrary SMTP command injection.

Patches

It is recommended that the Nextcloud Server is upgraded to 22.2.8 , 23.0.5 or 24.0.1.
It is recommended that the Nextcloud Enterprise Server is upgraded to 19.0.13.7, 20.0.14.6, 21.0.9.5, 22.2.8 or 23.0.5.

Workarounds

No workaround available

References

- HackerOne
- PullRequest

For more information

If you have any questions or comments about this advisory:

- Create a post in nextcloud/security-advisories
- Customers: Open a support ticket at support.nextcloud.com

Severity

Moderate **4.1** / 10

CVSS base metrics

Attack vector	**Network**
Attack complexity	**Low**
Privileges required	**Low**
User interaction	**Required**
Scope	**Changed**
Confidentiality	**None**
Integrity	**Low**
Availability	**None**

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

CVE ID

CVE-2022-31014

Weaknesses

CWE-93

Credits

 **spaceraccoon**