XMind Man-in-the-Middle

contact@rampartssecurity.com

Contents

1. Introduction

XMind is the "Most Popular Mind Mapping Tool" with "Millions of people" using it to "clarify thinking, manage complex information, run brainstorming and get work organized."[1]

It is a software program written in Java and designed to run on Windows, OSX, and Linux. There are several versions of the program[2], one of which is completely free.

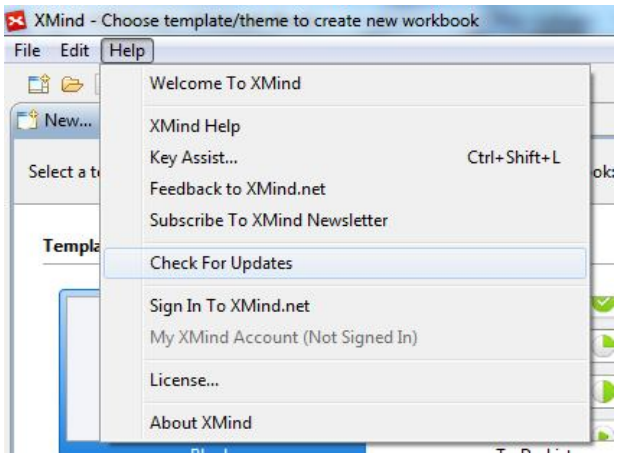
In response to XMind's bug bounty program[3], we briefly evaluated the network security of the free version of the application on Windows. We found the program is vulnerable to arbitrary remote code execution.

[1] http://www.xmind.net/
[2] http://www.xmind.net/pricing/
[3] http://www.xmind.net/bugbounty/

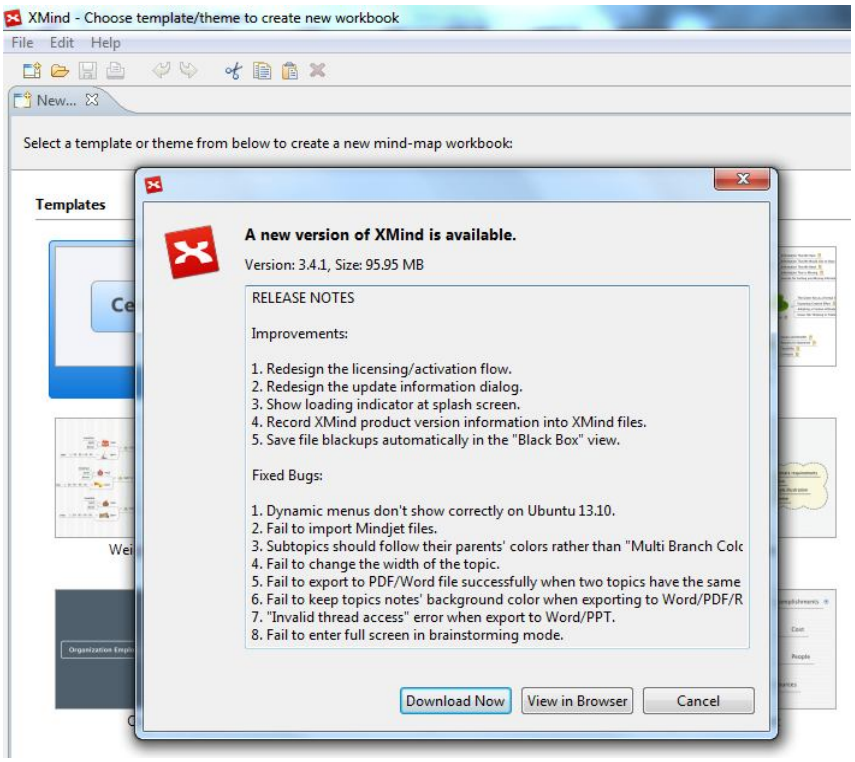
2. Attack

2.1 Update Process

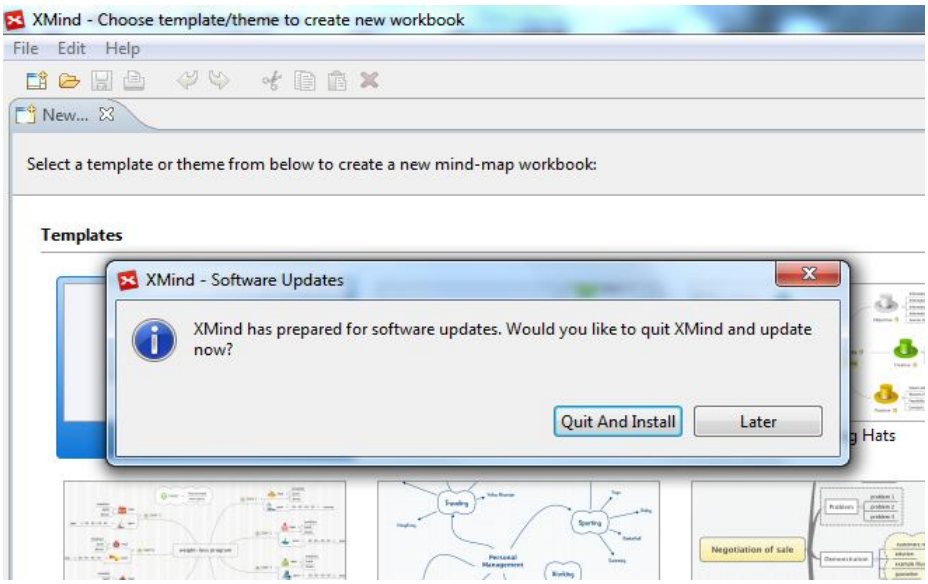
Like most software packages, XMind includes functionality to update their software.



Once the user has clicked "Check For Updates", XMind sends an HTTP GET request to the update server with its software version as a URL parameter. The update server responds with a URL to a newer version if one exists. The user is prompted if they would like to download the newer version.



When the user selects "Download Now", XMind automatically downloads the newer version. The user is then prompted if they would like to install now.

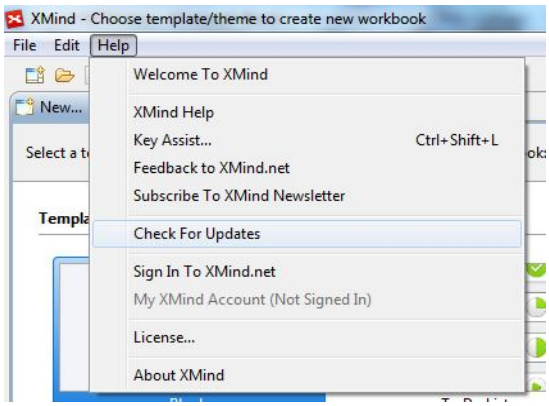


All of the communication between XMind and the update server is done over HTTP.

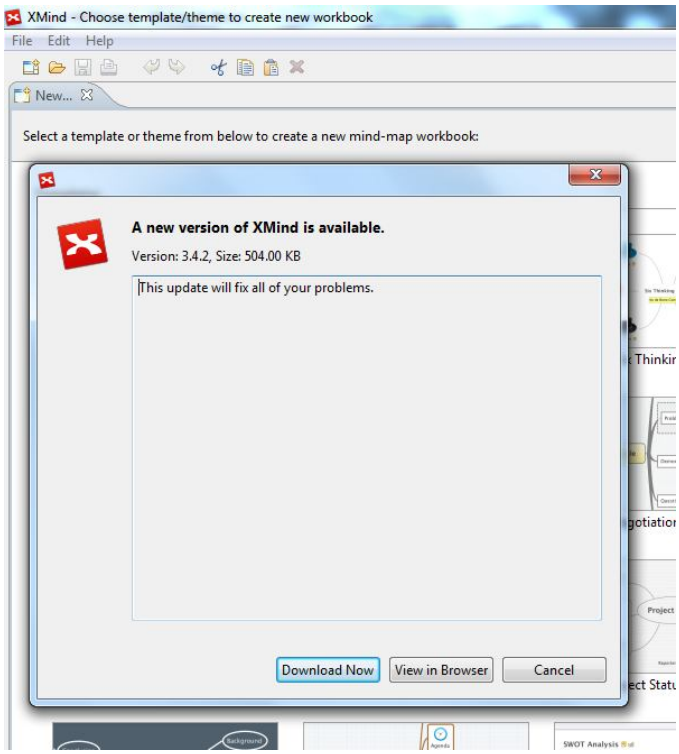
2.2 CVE-2014-2680

An appropriately positioned attacker can exploit a victim by acting as a man-in-the-middle during the update process. When an update check is done by XMind, an attacker can indicate an update is available and respond with arbitrary code as the update. This has been issued CVE-2014-2680[4].

As before, a victim initiates an update.

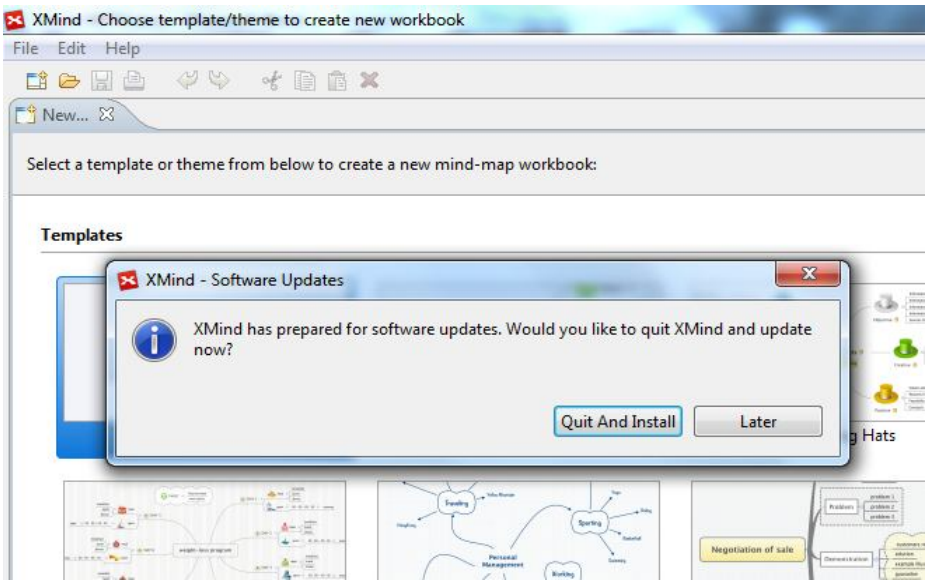


The attacker responds with a URL to a newer version. The user is prompted if they would like to download the newer version.

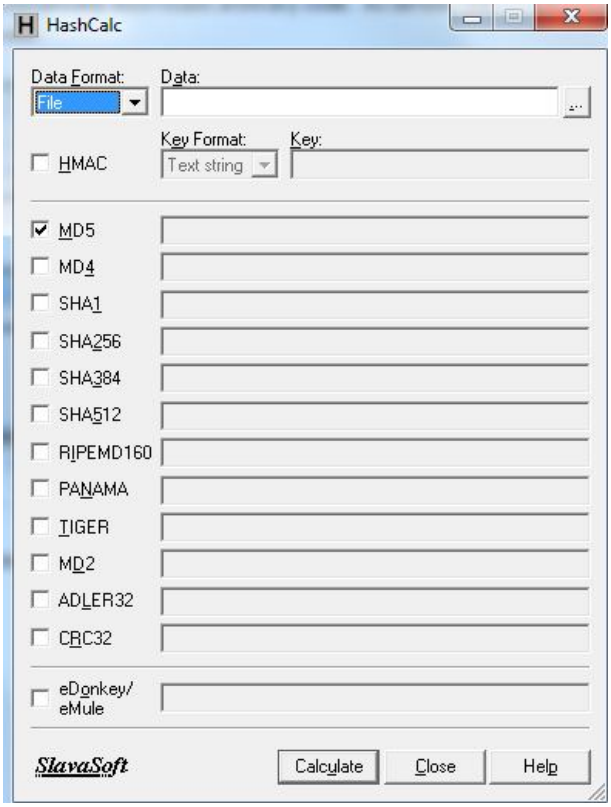


[4] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2680

When the user selects "Download Now", XMind automatically downloads the arbitrary code. As before, the user is then prompted if they would like to install now.



XMind then exits and the arbitrary code is run. In this instance, we've chosen to run HashCalc[5].



[5] http://www.slavasoft.com/hashcalc/

3. Recommendations

3.1 End User

1. Do not update XMind from within the program. Only update XMind by visiting the web site directly.

3.2 Vendor

1. Only retrieve updates over HTTPS.

This helps to ensure the update package is coming from the XMind server.

2. Sign all update packages.

During an update, XMind should verify the validity of an update package using an attached digital signature.

4. Timeline

1/20/2014	Vulnerability discovered
2/15/2014	1st notification to vendor
3/2/2014	2nd notification to vendor
3/3/2014	3rd notification to vendor
4/7/2014	US-CERT contacted
4/23/2014	Report published