swordbytes / **Advisories** Public

Code Issues Pull requests Actions Projects Security Insights

master

Advisories / 2021 / Advisory_CVE-2021-33501.pdf

Niemand Added CVE-2021-33501 PDF version **History**

0 contributors

533 KB

SWORDBYTES

PROTECTING YOUR GAMING EXPERIENCE

Overwolf 1-Click Remote Code Execution

CONFIDENTIAL DOCUMENT - ADVISORY ID INTERNAL SB-2021-0010

Table of Contents

Table of Contents

1. Advisory Information

Title: Overwolf 1-Click Remote Code Execution
Date published: 2021-05-31
Vendor: Overwolf Ltd
Release mode: Coordinated Release
Credits: This vulnerability was discovered and researched by Joel Noguera.

2. Vulnerability Information

Class: CWE-94 - Improper Control of Generation of Code ('Code Injection')
Severity: Critical - 9.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
Remotely exploitable: Yes
Locally exploitable: Yes
Affected version(s): Overwolf Client 0.169.0.22 (prior versions might also be affected)
CVE ID: CVE-2021-33501

3. Vulnerability Description

SwordBytes researchers have identified an Unauthenticated Remote Code Execution (RCE) vulnerability in Overwolf's Client Application by abusing a Reflected Cross-Site Scripting (XSS)

issue present in the *"overwolfstore://"* URL handler. This vulnerability allows remote unauthenticated attackers to execute arbitrary commands on the underlying operating system that hosts Overwolf's Client Application. By combining the XSS issue with a Chromium Embedded Framework (CEF) sandbox escape, it is possible for attackers to achieve Remote Code Execution on the victim's computer.

SwordBytes used the following Proof of Concept to achieve Remote Code Execution:

Proof of Concept:

```
overwolfstore://app/apps/<img+src=x+onerror=%22overwolf.io.writeFileContents('C:\\windows\\temp\\d.bat','start%20cmd%20%252fk%20whoami','',false,console.log)%2526overwolf.utils.openUrlInDefaultBrowser('C:\\windows\\temp\\d.bat')%22>/CCCCCC
```

4. Technical Description

Windows applications can register custom URL schemes to the operating system, which allow them to run a particular installed application when invoked. A common example is to make use of this scheme directly from the browser by navigating to an URL using the custom scheme (e.g., *"overwolfstore://app/:uid/reviews/:commentId"*). In this case, attackers can achieve this by redirecting valid users to a malicious link that abuse the custom URL handler from Overwolf (*"overwolfstore://"*). The client application is vulnerable to Cross-Site Scripting injection attacks by abusing unintended behavior on the back-end.

The *"overwolfstore://"* custom scheme is registered by one of the built-in extensions called *"Overwolf Appstore"* (UID *ojgnfnbjckbpfaciphphehonokbggjhpnnoafack*), which is part of the core