SteamOS Vulnerability Catalog

@g1a55er

Introduction

This brief report analyzes the dependencies bundled with SteamOS v3.5.7 and Steam Client Build v1705108172 for potentially exploitable publicly known vulnerabilities. An earlier public report indicated that even new versions of SteamOS came bundled with outdated dependencies. I have built upon that work by searching more of SteamOS' exposed attack surface for bundled dependencies, surfacing many critical dependencies the previous report missed. I have filtered out reports that merely may pertain to the effected software versions down to a shorter, urgent list of critical and high rated vulnerabilities that the reports claim can defeat security measures on SteamOS as it is actually used.

Publicly Known Vulnerabilities

Methodology

I started by exploring SteamOS to find software dependencies that are rather than merely being part of the image, and that thus might expose some attack surface to exploit. I found that SteamOS is split into two separately distributed and updated components. First, there is the underlying **system** image, that contains the Arch Linux-based operating system and all its dependencies, which is distributed as a read-only rootfs image, Second, there is a Steam **client** app that makes up most of the user-facing interface. The Steam client app is a standard Linux application that runs on top of the system image, with most of the actual interface being written as a web-app running using the Chromium Embedded Framework (**CEF**). Thus, these are the three main places where bundled dependencies may live in SteamOS:

1) System-wide dependencies that are distributed with the system image are generally found in places like /usr/lib.
2) Dependencies bundled with the Steam Client app are generally found in ~/.steam/bin64.
3) CEF uses its own completely separate set of dependencies which it statically links into its own library, found at ~/.steam/bin64/libcef.so.

For each of these dependency stores, I looked for high-risk dependencies (e.g. image parsers, compression libraries, etc.) and checked if the bundled versions of those dependencies were up-to-date. If they were not up-to-date, I checked public vulnerability databases (e.g. https://nvd.nist.gov/ or https://www.cvedetails.com/) to see if there were any publicly disclosed high or critical severity vulnerabilities. For each vulnerability, I read the report and compared it to the configuration of that vulnerability in SteamOS to try and infer whether the vulnerability posed an issue to SteamOS' security. I heavily favored manual analysis over automated analysis, to ensure that I produced high-quality actionable findings.

Findings

Client Dependency - Chromium Embedded Framework

By far, the biggest practical security risk is the outdated CEF library bundled with the Steam client app. It is version 85.0.4183.121, which was released in September 2020.

CVEDetails.com's database lists 1,037 total vulnerabilities affecting this outdated version at the time of this writing.

I filtered that to vulnerabilities that met the following criteria:

- Remote Code Execution (RCE) vulnerabilities
- Listed in the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) list, and that
- Appeared by manual inspection of the report description to be exploitable via the Steam client app's attack surface.

I excluded sandbox escape vulnerabilities because the Steam client's CEF instance runs without the sandbox enabled.

This left a list of 29 likely exploitable serious vulnerabilities, of which Valve only patched one[1] after I contacted them highlighting the outdated CEF version. The other 28 likely exploitable serious vulnerabilities are listed below:

Vulnerability	CVSS	CISA KEV?	Public Report Link
CVE-2021-21224	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-2
CVE-2024-0519	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2024-0
CVE-2023-7024	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2023-7
CVE-2023-4863	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2023-4
CVE-2023-4762	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2023-4
CVE-2023-3079	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2023-3
CVE-2023-2033	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2023-2
CVE-2022-4262	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-4
CVE-2022-3723	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-3
CVE-2022-3038	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-3
CVE-2022-2294	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-2
CVE-2022-1364	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-1
CVE-2022-1096	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-1
CVE-2022-0609	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2022-0
CVE-2021-38003	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-3
CVE-2021-37975	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-3

[1] Valve patched CVE-2020-16040 in their bundled libcef.so after I contacted them via Hacker One with a demonstration exploit.

Vulnerability	CVSS	CISA KEV?	Public Report Link
CVE-2021-30632	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-3
CVE-2021-30563	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-3
CVE-2021-30554	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-3
CVE-2021-30551	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-3
CVE-2021-21220	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-2
CVE-2021-21206	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-2
CVE-2021-21193	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-2
CVE-2021-21166	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-2
CVE-2021-21148	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-2
CVE-2021-4102	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2021-4
CVE-2020-16013	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2020-1
CVE-2020-16009	8.8 / HIGH	Y	https://www.cvedetails.com/cve/CVE-2020-1

Other Client Dependencies

I also manually checked the versions of the other dependency libraries bundled with the Steam client against public reports in vulnerability databases. I found two high priority CVEs listed. These vulnerabilities should be fixed, but they don't seem nearly as immediately exploitable as the CEF vulnerabilities listed above. This is just more evidence to emphasize the point that the CEF dependency being out of date is not a one-off issue; the Steam client bundled multiple out of date dependencies.

Vulnerability	Component	Component Version	CVSS	Report Link
CVE-2023-5217	libvpx	1.10.1	8.8 / HIGH	https://www.cvede
CVE-2021-30123	libavcodec (ffmpeg)	58.91.100 (4.3.4)	8.8 / HIGH	https://www.cvede

System Dependency - Linux Kernel Vulnerabilities

The version of SteamOS I investigated includes a fork of the Linux kernel based on kernel version 6.1.52. You can browse the source code for this fork here. I checked public vulnerability databases to find a few high severity kernel vulnerabilities that could be used to achieve LPE even in the absence of the misconfiguration I discovered, and I found at least four candidates, listed below:

Vulnerability	CVSS	Public Report Link
CVE-2024-1086	7.8 / HIGH	https://www.cvedetails.com/cve/CVE-2024-1086/
CVE-2023-5197	7.8 / HIGH	https://www.cvedetails.com/cve/CVE-2023-5197/
CVE-2023-4244	7.8 / HIGH	https://www.cvedetails.com/cve/CVE-2023-4244/
CVE-2023-5345	7.8 / HIGH	https://www.cvedetails.com/cve/CVE-2023-5345/

Other System Dependencies

The previous report focused on dependencies bundled with the operating system, and there are indeed a handful of highly rated vulnerabilities in high-risk dependencies there. However, based on the attack surface these components actually expose to malicious actors, I don't believe they actually pose a serious practical threat to normal users. For example, the libvpx vulnerability requires getting the vulnerable software to encode video with attacker-controlled encoding settings, but I could not really see a place where that could be exploited, as most web browsers bring their own libvpx. As a second example, the OpenSSH vulnerability is very highly rated, but it similarly requires the user to forward their ssh-agent to an attacker controlled system, which is an unlikely behavior for the vast majority of users of a gaming console.

The main issue with these vulnerabilities is that they are another sign that outdated dependencies linger in SteamOS for some time.

Vulnerability	Component	Component Version	CVSS	Report Link
CVE-2023-4863	libwebp	1.3.0	8.8 / HIGH	https://www.cvede
CVE-2023-5217	libvpx	1.13.0	8.8 / HIGH	https://www.cvede
CVE-2023-38408	OpenSSH	9.3p1	9.8 / CRITICAL	https://www.cvede

Conclusion

In total, this report identifies 37 publicly known potentially exploitable high or critical severity scored vulnerabilities present in recent versions of SteamOS. These vulnerabilities present an abundant opportunity to easily and cheaply craft exploits to attack SteamOS and its users, which I demonstrate with my example rootkit and exploit chain.