Date: Tue, 9 Feb 2021 07:36:15 +0100
From: Salvatore Bonaccorso <carnil@...ian.org>
To: oss-security@...ts.openwall.com
Subject: Re: [cve-pending] Firejail: root privilege escalation
 in OverlayFS code

Hi,

On Mon, Feb 08, 2021 at 02:15:05PM +0000, netblue30 wrote:
>
> Security Advisory - Feb 8, 2021
>
> Summary: A vulnerability resulting in root privilege escalation was discovered in Firejail's OverlayFS code,
>
> Versions affected: Firejail software versions starting with 0.9.30.
> Long Term Support (LTS) Firejail branch is not affected by this bug.
>
> Workaround: Disable overlayfs feature at runtime. In a text editor open /etc/firejail/firejail.config file,
> and set "overlayfs" entry to "no".
>
> $ grep overlayfs /etc/firejail/firejail.config
>   # Enable or disable overlayfs features, default enabled.
>   overlayfs no
>
> Fix: The bug is fixed in Firejail version 0.9.64.4
>
> GitHub commit: (file configure.ac)
> https://github.com/netblue30/firejail/commit/97d8a03cad19501f017587cc4e47d8418273834b
>
> Credit: Security researcher Roman Fiedler analyzed the code and discovered the vulnerability.
> Functional PoC exploit code was provided to Firejail development team.
> A description of the problem is here on Roman's blog:
>
> https://unparalleled.eu/publications/2021/advisory-unpar-2021-0.txt
> https://unparalleled.eu/blog/2021/20210208-rigged-race-against-firejail-for-local-root/

CVE-2021-26910 was assigned for this issue according to
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26910 .

Regards,
Salvatore