

# USN-4738-1: vulnerabilities

## OpenSSL

Paul Kehrer discovered that OpenSSL incorrectly handled certain input lengths in EVP functions. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2021-23840)

Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer fields. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2021-23841)

---

# USN-4737-1: vulnerability

## Bind

It was discovered that Bind incorrectly handled GSSAPI security policy negotiation. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly execute arbitrary code. In the default installation, attackers would be isolated by the Bind AppArmor profile.

---

# Change the sort-order in Lubuntu Quick Launch

Lubuntu has gone from LXDE to LXQt. In LXQt there's no way to drag the icons in the quick launch to sort them to your liking. Fear not, you can still sort them.

This one is actually pretty easy, you just have to know where to look.

**Edit:** Press and hold CTRL and then you can drag and drop them...

Navigate to `~/.config/lxqt/` and open 'panel.conf' with your favorite text editor. Scroll down until you see:

```
[quicklaunch]
```

You'll then see your quick-launch applications on their own line and they'll have a numeric value. That numeric value is how you sort them.

For example, mine looks like this:

```
[code]apps\1\desktop=/usr/share/applications/pcmanfm-qt.desktop
apps\2\desktop=/usr/share/applications/xfce4-terminal.desktop
apps\3\desktop=/usr/share/applications/filezilla.desktop
apps\4\desktop=/usr/share/applications/chromium-browser.desktop
apps\5\desktop=/usr/share/applications/thunderbird.desktop
apps\6\desktop=/usr/share/applications/google-chrome.desktop[/code]
```

In the 'apps\1\desktop' there is a 1. That translates to the furthest right icon in the quick launch area of the taskbar. If I wanted it to be on the furthest left, I'd change the 1 to a 6 and then change something else to be 1. It's pretty

straightforward. I was pleasantly surprised when I was able to find that section. Why we can't just drag them around like we could on LXDE is another matter entirely.

As always, scroll on up and subscribe to get notifications when I publish something new. Or not... It's up to you! Who the heck am I to be shouting out orders anyhow?!?

---

# **DARPA and the Linux Foundation Create Open Software Initiative to Accelerate US R&D Innovation, 5G End to End Stack**

- *Partnership enables acceleration of innovation, collaboration, and US competitiveness in areas of 5G, Edge, IOT, AI and Security*
- *New umbrella organization at the Linux Foundation, US GOV OPS, to host first project, OPS 5G (Open Programmable, Secure), to accelerate 5G, Edge & IoT technologies creation and deployment*
- *Open Ecosystem efforts aligns on a common open source architecture and set of open source projects and focuses on integrations and enhancements to the secure open source end to end 5G stack.*
- *Effort leverages the existing networking open source projects and community efforts at the Linux Foundation*

*and industry disruptions like disaggregation, SDN/NFV, and cloud native.*

**SAN FRANCISCO – February 17, 2021** – The Linux Foundation (LF), the nonprofit organization enabling mass innovation through open source, today announced it has signed a collaboration agreement with the Defense Advanced Research Projects Agency (DARPA) to create open source software that accelerates United States government technology research and development innovation.

Under the agreement, DARPA and the LF will create a broad collaboration umbrella (US Government Open Programmable Secure (US GOV OPS) that allows United States Government projects, their ecosystem, and open community to participate in accelerating innovation and security in the areas of 5G, Edge, AI, Standards, Programmability, and IOT among other technologies. The project formation encourages ecosystem players to support US Government initiatives to create the latest in technology software.

The project will launch as a standard open source project with neutral governance and a charter similar to other projects within the Linux Foundation. Additionally, the agreement enables collaboration with upstream and downstream communities such as LF Networking, LF Edge, and Zephyr, among others, to build on a secure code base for use by the US Government.

“DARPA’s use of open source software in the Open Programmable Secure 5G (OPS-5G) program leverages transparency, portability and open access inherent in this distribution model,” said Dr. Jonathan Smith, DARPA Information Innovation Office Program Manager. “Transparency enables advanced software tools and systems to be applied to the code base, while portability and open access will result in decoupling hardware and software ecosystems, enabling innovations by more entities across more technology areas.”

“We are eager to ally with DARPA and its intent to accelerate secure, open source innovation and US competitiveness across breakthrough technologies,” said Arpit Joshipura, general manager, Networking, Edge, & IOT, the Linux Foundation. “This partnership enables transformational change across open software and systems, leveraging the best shared resources across the ecosystem.”

The new US GOV OPS umbrella will include the Open Programmable Secure- 5G (OPS-5G) program as its first project, currently in formation with the help of DARPA, the US Navy and additional performers. The goal of OPS-5G is to create open source software and systems enabling secure end to end 5G and follow-on mobile networks. OPS-5G will create capabilities to address feature velocity in open source software, mitigating large scale Botnet of Things (BoT), network slicing on suspect gear, and adaptive adversaries operating at scale.

DARPA’s Dr. Jonathan Smith will be presenting at the upcoming Open Networking and Edge Executive Forum (ONEEF) a virtual event taking place March 10-12. This special Executive Edition of Open Networking & Edge Summit, the industry’s premier open networking & edge computing event, will feature executive leadership across the networking and edge ecosystems sharing their visions with a global audience in the Telco, Cloud and Enterprise verticals.

To learn more about US GOV OPS and OPS-5G, please visit [www.usgovops.org](http://www.usgovops.org).

### **About the Linux Foundation**

Founded in 2000, the Linux Foundation is supported by more than 1,000 members and is the world’s leading home for collaboration on open source software, open standards, open data, and open hardware. Linux Foundation’s projects are critical to the world’s infrastructure including Linux, Kubernetes, Node.js, and more. The Linux Foundation’s

methodology focuses on leveraging best practices and addressing the needs of contributors, users and solution providers to create sustainable models for open collaboration. For more information, please visit us at [linuxfoundation.org](https://linuxfoundation.org).

###

*The Linux Foundation has registered trademarks and uses trademarks. For a list of trademarks of The Linux Foundation, please see our trademark usage page: <https://www.linuxfoundation.org/trademark-usage>. Linux is a registered trademark of Linus Torvalds.*

The post DARPA and the Linux Foundation Create Open Software Initiative to Accelerate US R&D Innovation, 5G End to End Stack appeared first on Linux Foundation.

---

## **USN-4734-2: wpa\_supplicant and hostapd vulnerabilities**

USN-4734-1 fixed several vulnerabilities in wpa\_supplicant. This update provides the corresponding update for Ubuntu 14.04 ESM. It was discovered that wpa\_supplicant did not properly handle P2P (Wi-Fi Direct) group information in some situations, leading to a heap overflow. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-0326)

It was discovered that hostapd did not properly handle UPnP

subscribe  
messages in some circumstances. An attacker could use this to  
cause a  
denial of service. (CVE-2020-12695)