Security Advisory 2024-103

Critical Vulnerabilities in CUPS

September 27, 2024 — v1.0

TLP:CLEAR

History:

- *27/09/2024 — v1.0 – Initial publication*

Summary

On September 26, 2024, a security researched released a blog post describing several vulnerabilities in CUPS, one of which being critical, allowing an attacker to replace existing printers' IPP URLs with a malicious one, resulting in a potential arbitrary command execution [1].

Technical details

By chaining the vulnerabilities (**CVE-2024-47076**, **CVE-2024-47175**, **CVE-2024-47176** and **CVE-2024-47177**) together, an attacker could potentially achieve remote code execution [1].

Exploitation of these vulnerabilities is possible through the following chain of events:

1. The `cups-browsed` service has been enabled or started.
2. An attacker has access to a vulnerable server, which:
   - allows unrestricted access, such as the public internet, or
   - gains access to an internal network where local connections are trusted.
3. Attacker advertises a malicious IPP server, thereby provisioning a malicious printer.
4. A potential victim attempts to print using the malicious device.
5. Attempted printing allows the attacker to execute arbitrary code on the victim's machine.

Affected products

This group of vulnerabilities affects most of the Linux systems.

You can determine if `cups-browsed` is running by running the following command:

```
sudo systemctl status cups-browsed
```

Recommendations

CERT-EU recommends reviewing and applying the patches from Linux distribution security bulletins, including but not limited to:

- Ubuntu [2]
- RedHat [3]

CERT-EU also recommends to disable the `cups-browsed` service in any environment where printing is not needed, or patches are not yet available, using the following commands:

```
sudo systemctl stop cups-browsed
sudo systemctl disable cups-browsed
```

References

[1] https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/

[2] https://ubuntu.com/security/notices/USN-7042-1

[3] https://www.redhat.com/en/blog/red-hat-response-openprinting-cups-vulnerabilities