National Cyber Security Centre

2409260163-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerabilities in Red Hat Enterprise Linux OpenPrinting CUPS

(CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CVE-2024-47177)

Friday 27th September, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Red Hat has disclosed details of a group of vulnerabilities (CVE-2024-47076, CVE-2024-47175, CVE-2024-47176 and CVE-2024-47177) within OpenPrinting CUPS, an open source printing system that is prevalent in most modern Linux distributions, including Red Hat Enterprise Linux (RHEL).

CUPS provides tools to manage, discover and share printers for Linux distributions. By chaining this group of vulnerabilities together, an attacker could potentially achieve remote code execution which could then lead to theft of sensitive data and/or damage to critical production systems.

Red Hat rates these issues with a severity impact of Important. While all versions of RHEL are affected, **affected packages are not vulnerable in their default configuration**. At this time, there are four CVEs assigned to these vulnerabilities, but the exact number is still being coordinated with the upstream community and the researcher who discovered the problem.

Products Affected

- All versions of Red Hat Enterprise Linux (RHEL)

Detection

Red Hat customers should use the following command to determine if cups-browsed is running:

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

If the result includes “Active: inactive (dead)” then the exploit chain is halted and the system is not vulnerable.

If the result is “running” or “enabled,”and the “BrowseRemoteProtocols” directive contains the value “cups” in the configuration file /etc/cups/cups-browsed.conf, then the system is vulnerable.

Mitigation

To stop a running cups-browsed service, an administrator should use the following command:

```
$ sudo  systemctl stop cups-browsed
```

The cups-browsed service can also be prevented from starting on reboot with:

```
$ sudo systemctl disable cups-browsed
```

Red Hat and the broader Linux community are currently working on patches to address these issues. Please see the below links for further information:

- https://www.redhat.com/en/blog/red-hat-response-openprinting-cups-vulnerabilities?sc_cid=701f2000000tyBjAAI
- https://ubuntu.com/security/notices/USN-7042-1
- https://security-tracker.debian.org/tracker/CVE-2024-47176

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre