CYBER ADVISORY

TLP:CLEAR

30 SEP 2024

Common UNIX Printing System (CUPS) Multiple Vulnerabilities

CUPS | Multiple CVEs | Remote Code Execution | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical vulnerabilities affecting Common UNIX Printing System (CUPS). Exploitation of these vulnerabilities could potentially allow an attacker the ability to replace/install new or existing printers Internet Printing Protocol (IPP) Uniform Resource Locator (URLs) with a malicious one, resulting in remote command execution when a print job is started from that computer.[1]

Affected Vendor	Affected Product	Issue	CVE Identifier(s)	CVSS v3.1
OpenPrinting	Libscupsfilters **Versions up to and including 2.1b1**	Improper Input Validation or Sanitization Vulnerability Is a flaw in the libcupsfilters library in which IPP packets are not validated or sanitized. This provides the attacker the ability to send malicious data to the CUPS system.	**CVE-2024-47076**	**8.6 High**
	Libppd **Versions up to and including 2.1b1**	Improper Input Validation or Sanitization Vulnerability IPP data is not properly validated or sanitized before being written to a temporary PostScript Printer Description (PPD) file. This can result in an attacker injecting malicious data into the PPD file.	**CVE-2024-47175**	**8.6 High**
	Cups-browsed **Versions up to and including 2.0.1**	Binding to an Unrestricted IP Address Vulnerability. This bug affecting the cups-browsed library allows any packet from any source to be trusted on the IPP port (default 631). Because of this, an attacker could send a crafted packet that would trigger	**CVE-2024-47176**	**8.4 High**

		a **Get-Printer-Attributes IPP** request, which would then reach out to an attacker controller URL.		
	Cups-filters **Versions up to and including 2.0.1**	Command Injection Vulnerability Impacts the cups-filters library and could allow an attacker to execute arbitrary commands using "via the FoomaticRIPCommandLine PPD parameter."	**CVE-2024-47177**	**9.1 High**

Table 1: Vulnerable CUPS Products[2]

The Cal-CSIC recommends immediately upgrading all affected to the latest CUPS Packaged based on your vendor specific system.[3]

For further information on upgrading affected CUPS products, please refer to CUPS | OpenPrinting cups-filters Red Hat.

Organization, Source, Reference, and Dissemination Information	
Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Security Boulevard; "CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CVE-2024-47177: Frequently Asked Questions About Common UNIX Printing System (CUPS) Vulnerabilities;" https://securityboulevard.com/2024/09/cve-2024-47076-cve-2024-47175-cve-2024-47176-cve-2024-47177-frequently-asked-questions-about-common-unix-printing-system-cups-vulnerabilities/; accessed 30 September 2024

[2] Wiz; "CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CVE-2024-47177: Everything you need to know;" https://www.wiz.io/blog/openprinting-cups-vulnerabilities-cve-2024-47076-cve-2024-47175-cve-2024-47176-cve-2024-47177; accessed 30 September 2024

[3] Evilsocket; "Attacking UNIX Systems via CUPS, Part I;" https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/; accessed 30 September 2024