Release 3, July 2024

What's New in Release 3, July 2024

Table 1: What's New in July 2024

Feature	Description
Security Fix for CVE-2024-6387	The vulnerability is related to remote, unauthenticated code execution and affects the OpenSSH server (sshd) in glibc-based Linux systems. The vulnerability is a race condition in the signal-handling mechanism. A race condition occurs when the behavior of software depends on the sequence or timing of uncontrollable events such as signals. This condition can lead to unpredictable behavior or security issues. For more information, see CVE-2024-6387.

Note To upgrade to Release 3 July 2024, refer to Upgrade Path for Release 3 section.

Restriction This release does not support inline upgrade due to the open issue CSCwk38085. We recommend that you download the new connector image from CCO, and upgrade your connectors to address the vulnerability, using the connectoros upgrade *.connector-image* command.

Issues

Open Issues in Release 3, July 2024

Table 2: Open Issues

ID	Description
CSCwk38085	Download of Connector image fails when the system inline upgrade is triggered from GUI or CLI.

Resolved Issues in Release 3, July 2024

Table 3: Resolved Issues

ID	Description
CSCwk37982	Docker does not shut down gracefully during system inline upgrades.
CSCwk62273	Evaluation of Cisco Spaces for OpenSSH regreSSHion vulnerability.