PitStop Library Container 2325

Release notes

ENFOCUS

Public

Contents

What's new?

In this version, we worked on reducing the level of vulnerabilities to increase PLC security. It was an important effort that we made to ensure that our customers benefit from the highest level of security.

1. OS update

We updated the PLC OS to Ubuntu 23.04.

2. Node.js update

We updated NPM to version 9.7.1 and Node.js to version 20.

3. Issues fixed

In this version, a series of vulnerability issues were fixed. You can find the complete list here:

CVE-2022-33987	**Medium**	The got package before 12.1.0 (also fixed in 11.8.5) for Node.js allows a redirect to a UNIX socket.
CVE-2022-25881	**High**	This affects versions of the package http-cache-semantics before 4.1.1. The issue can be exploited via malicious request header values sent to a server, when that server reads the cache policy from the request using this library.
CVE-2023-28155	**Medium**	** UNSUPPORTED WHEN ASSIGNED ** The Request package through 2.88.1 for Node.js allows a bypass of SSRF mitigations via an attacker-controller server that does a cross-protocol redirect (HTTP to HTTPS, or HTTPS to HTTP). NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2021-3807	**High**	ansi-regex is vulnerable to Inefficient Regular Expression Complexity

Creating a vulnerability report is now part of our standard work to ensure vulnerabilities are detected as soon as they are introduced.

Bug fixes

The following bugs have been reported and fixed in this version:

ENFCLOUD-816	Providing the error message in the logs if fixed file or report is failed to upload to the location.