Advisory	**EXX-2021-02**		April 26, 2021
Manufacturer	pixx.io GmbH	Product	pixx.io
Affected Version(s)	Before 1.11	Tested Version(s)	1.11
CWE	CWE-23: Relative Path Traversal	CVE	–
Risk	High	Status	Closed

Overview

pixx.io is a platform for managing and providing media. This can be operated on-premise or in the manufacturer's cloud.

The manufacturer describes the product as follows [1] :
"Mit pixx.io schneller und genial einfach mit digitalen Medien arbeiten: Speichern und organisieren Sie Ihren Medienpool zentral - jederzeit und überall verfügbar."

However, due to e insufficient validation of the media paths, an attacker can retrieve any file from the server.

Vulnerability Details

Files in web applications are often referenced by their relative path in a directory.

If an attacker has the ability to manipulate the path to a file and its name, he or she can try to read other files. In the worst case, this is even possible beyond the own directory. The attacker can try to use an absolute path instead of a relative one or jump up the directory tree using the control sequence "../" until the root directory is reached.

In the root directory, the attacker can then also read all files to which the web application user has read permissions.

Proof of Concept (PoC)

To exploit this vulnerability, an attacker without further authorization can send the following HTTP GET request :

https://vulnerable.host/workspace/pixxio/tt.php?dataPath=/pixxiodata/../&src=[FILE]

"[FILE]" in the URL has to be replaced by the path and the file name the attacker want to obtain (e.g. /etc/passwd). Since no folder contents are displayed, the attacker has to "guess" the files. However, if the file exists, it will be displayed in the browser or offered for download.

Solution

According to the manufacturer, the reported security issues has been fixed in version 1.12.0. Update your pixx.io instance to the latest version.

Disclosure Timeline

2021-04-08	Discovery of the vulnerability
2021-04-08	Notification of the manufacturer
2021-04-20	Patch release by the manufacturer
2021-04-26	Publication of the Advisory

References

[1] pixx.io homepage
https://www.pixxio-bildverwaltung.de/

[2] EXXETA homepage
https://www.exxeta.com

Credits

This security vulnerability was found by Florian Weller of EXXETA.
E-Mail: florian.weller@exxeta.com

Disclaimer

The information in this security advisory are a snapshot and without warranty of any kind. In order to provide the best possible accuracy, details of the advisory may be updated, The latest version of this security advisory is available on the EXXETA website [2] .

Copyright