Multiple Vulnerabilities in Pixera < 25.2 R3

Summary

Two security issues were found in Pixera Two Media Server allowing attackers on the network to take control over the server via remote code execution which is allowed from the default configuration.

1. Remote Code Execution (RCE) in Pixera Two Media Server
2. Arbitrary File Read in Pixera Two Media Server

Affected Products

- Model: Pixera Two Media Server
- Software Version: < 25.2 R3

Mitigation

1. Update to Pixera version 25.2 R3, released on 14 Oct 25. In this version, Pixera introduced API allow-listing, defaulting to restricted APIs rather than all enabled. Extra care should be taken when allow-listing sensitive APIs such as filesystem, web-related, and system utility APIs.
    - Reference: https://help.pixera.one/changelogs-version-overviews/pixera-252-overview-changelog#:~:text=Allowlist%20(accessible%20via%20top%20bar)%20to%20limit%20API%20access

    - Note: It appears Pixera's version format has changed over time. Previously, it used 2.0.XXX. Now it seems to use the year of release plus a minor version and revision number such as 25.2 R3.
2. Apply strict IP whitelisting, such that the web panel and API can only be accessed from dedicated, trusted sources.

Vulnerability 1 – Remote Code Execution

1.1. Description

An unauthenticated person with network access can obtain Remote Code Execution (RCE) by abusing the websocket API on the web server running on port 1338, which is open by default. This issue allows anyone on the network to take control of the Pixera media server, allowing them to run arbitrary commands, modify files, mine cryptocurrency, and pivot across connected networks.

1.2. PoC

WebSocket Payload:

```
{
    "type":"Request",
    "sequence":100,
    "address":"Utils.Redacted.redacted",
    "params":[
        "calc.exe",
        ""
    ]
}
```

Certain parts of the PoC have been redacted in the interest of security.

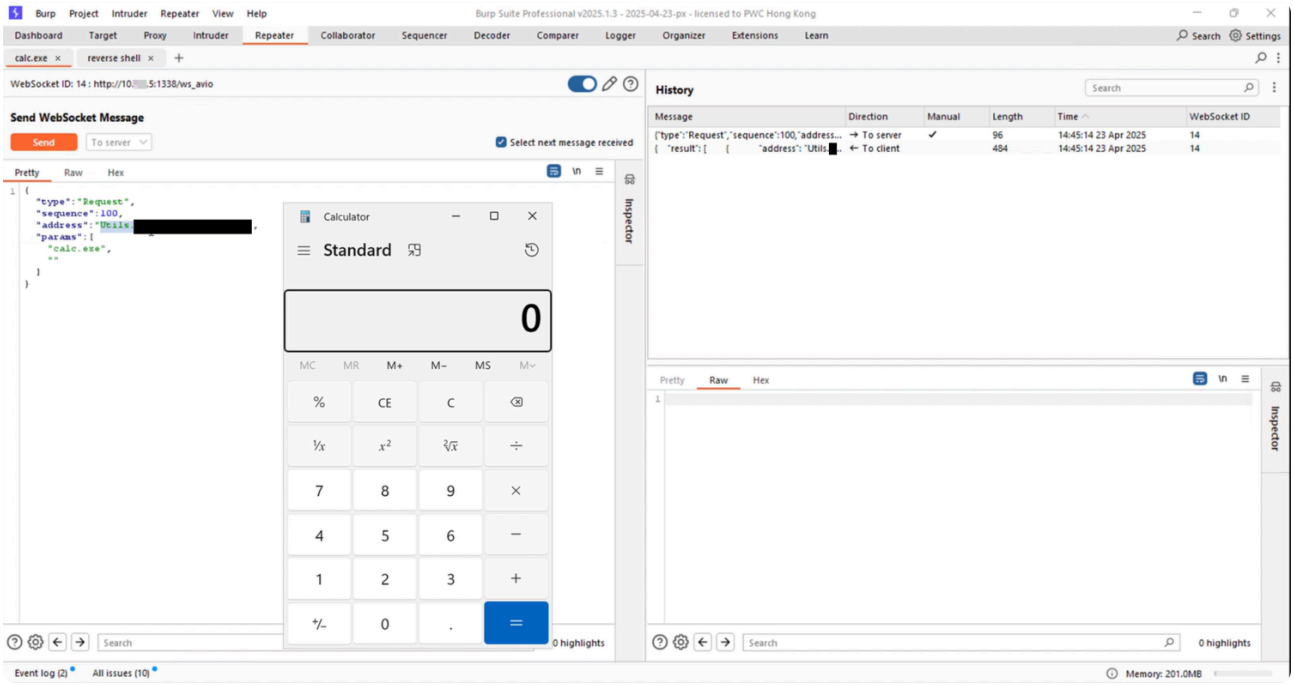

Figure 1A: Run calc.exe in a local deployment.

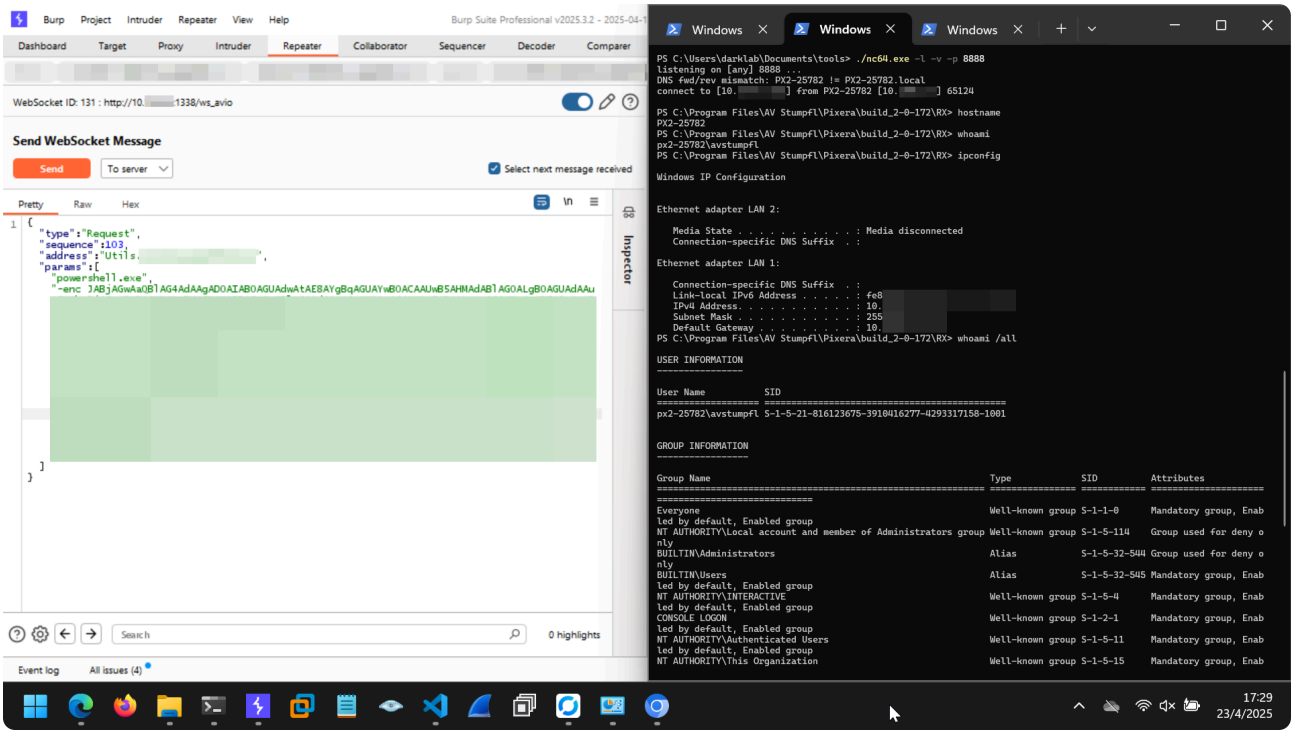

Figure 1B: Obtain a reverse shell in a remote deployment.

1.3. Impact

Commands are executed as the av-stumpfl user, which has Administrator privileges to the Windows server. Attackers can execute arbitrary commands on the media server, unlock further actions through UAC bypass, and pivot across the network.

1.4. Suggested CVSS

Suggested CVSS3 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Base Score: 9.4 (Critical)

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): None
- User Interaction (UI): None
- Scope (S): Unchanged
- Confidentiality Loss (C): Low
- Integrity Loss (I): High
- Availability Loss (A): High

Vulnerability 2 – Arbitrary File Read

2.1. Description

An unauthenticated person with network access can perform Arbitrary File Reads on the Pixera Media Server by targeting the web server hosted on port 1338. This allows anyone on the network to read any file on the Pixera media server.

2.2. PoC

```
http://TARGET:1338/..\..\..\..\..\..\windows\win.ini
```

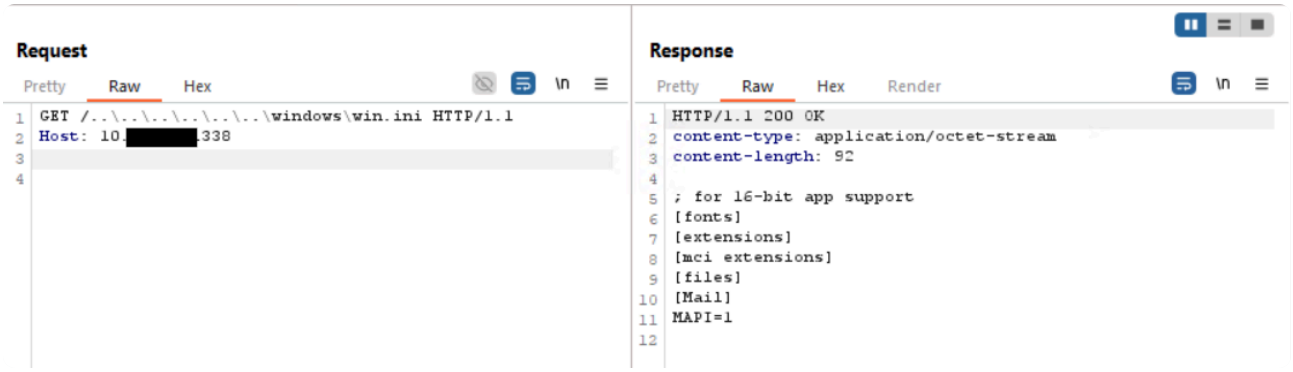

Figure 2A: Path traversal to win.ini

Figure 2B: Path traversal to a file containing build version.

2.3. Impact

The exploitation of this vulnerability can lead to unauthorized disclosure of information, potentially leading to system compromise. For instance, attackers may leverage this vulnerability to leak system files or registry data which may disclose login hashes to be cracked.

2.4. Suggested CVSS

Suggested CVSS3 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score: 5.3 (Medium)

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): None
- User Interaction (UI): None
- Scope (S): Unchanged
- Confidentiality Loss (C): Low
- Integrity Loss (I): None
- Availability Loss (A): None

Timeline

- 2025.07.04 - Vulnerability reported to AV Stumpfl
- 2025.07.28 - Report received by AV Stumpfl
- 2025.10.14 - Patch released (25.2 R3)
- 2026.04.15 - Disclosure to VulDB
- 2026.05.03 - VulDB publishes disclosure

Credit

- Johnathan Law from PwC HK DarkLab