

Communardo

SubSpace Navigation for Confluence Web Application
Penetration Test Report

Report creation date: **March 23, 2026**

Testing period: **February 11, 2026** to **March 19, 2026**

Prepared by: **Josh Durand**

CONFIDENTIAL INFORMATION • Do not share outside of organization

bugcrowd

Table of contents

Executive Summary 2
Engagement details 4
Findings table 5
F001 - No Rate Limiting on Create Menu Form 6
Reporting and Methodology 13
Appendix A - Risk and priority key 14
Appendix B - Vulnerability details 16
Closing Statement 17

Executive Summary

Communardo engaged Bugcrowd, Inc. to perform a Penetration Test that took place from February 11th, 2026, through March 19th, 2026.

The purpose of this engagement was to identify security vulnerabilities in the assets listed under the Targets and Scope section of the report. Once identified, each vulnerability was rated for technical impact defined in the Findings Summary.

Bugcrowd's testing methodology involves several key stages:

- Initial reconnaissance to gather critical information about the target environment,
- Enumeration to identify potential attack vectors,
- Exploitation to test the impact and feasibility of identified vulnerabilities, and
- Post-exploitation to evaluate the extent of potential compromise

The tester(s) used a number of sophisticated tools, techniques, and procedures for each of these stages. Crucially, our approach leverages human ingenuity, creative problem-solving, and critical thinking to uncover complex vulnerabilities that might otherwise go undetected from scanners and scripts alone. The insights gained from this assessment are intended to provide a comprehensive understanding of the organization's security risks, enabling informed decision-making and effective prioritization of remediation efforts.

At the time of this report, **1 vulnerabilities** were identified, including:

- **0 Critical**
- **0 Severe**
- **0 Moderate**
- **0 Low**
- **1 Informational**

At this time, **Bugcrowd has rated the risk to the Communardo's assets as Informational**. Our rating is based on the severity of the findings disclosed within this report.

It is recommended that Communardo focus on Critical and Severe vulnerabilities first, with Moderate, Low, and Informational findings being fixed once the most critical issues are remediated.

Bugcrowd recommends that all Critical, Severe, and Moderate severity findings are retested once remediation activities are completed.

If not already implemented, Bugcrowd recommends taking the following high-level actions to further improve the overall security posture of the organization:

- Implement a secure development lifecycle such as Microsoft Secure Development Lifecycle (MSDL).

- Implement a static code analysis (SAST) tool into the development lifecycle to minimize the introduction of vulnerabilities in code.
- Provide ongoing training to developers to ensure that they are aware of secure development practices and emerging threats.

The continuation of this report contains technical details of the specific vulnerabilities that were discovered throughout the Penetration Test.

This report is just a summary of the information available and is a 'snapshot' in time of the state for the tested environment.

All details of the engagement's findings — comments, code, and any researcher provided remediation information — can be found in the Bugcrowd Crowdcontrol platform: https://tracker.bugcrowd.com (https://tracker.bugcrowd.com)

Engagement details

Scope of testing

Prior to penetration test launching, Bugcrowd worked with Communardo. to define the rules of the engagement, commonly known as the engagement brief, which includes the scope of work.

The following targets were considered explicitly in-scope for testing:

- website: https://marketplace.atlassian.com/apps/1218247/sharepoint-connector-for-confluence?tab=overview
- website: https://marketplace.atlassian.com/apps/194/subspace-navigation-for-confluence?hosting=cloud&tab=overview

All details of the engagement scope and full brief can be reviewed in each of the respective Engagement Settings pages found on the Bugcrowd Crowdcontrol platform.

Findings table

The following table lists all validated findings identified through manual testing grouped by Vulnerability Rating Taxonomy (VRT):

Vulnerability Rating Taxonomy (VRT)	Title	Priority
Server Security Misconfiguration	F001 - No Rate Limiting on Create Menu Form	P5

Server Security Misconfiguration

P5

F001 - No Rate Limiting on Create Menu Form

Description

Rate limiting is a strategy to limit the frequency of a repeat action within a particular time frame. This ensures that a service doesn't become unresponsive or unavailable due to too many requests exhausting the application's resources. A lack of rate limiting on this endpoint allows an attacker to send a large number of requests to the server and potentially cause accelerated service usage for the business or exhaust the application resources.

Business Impact

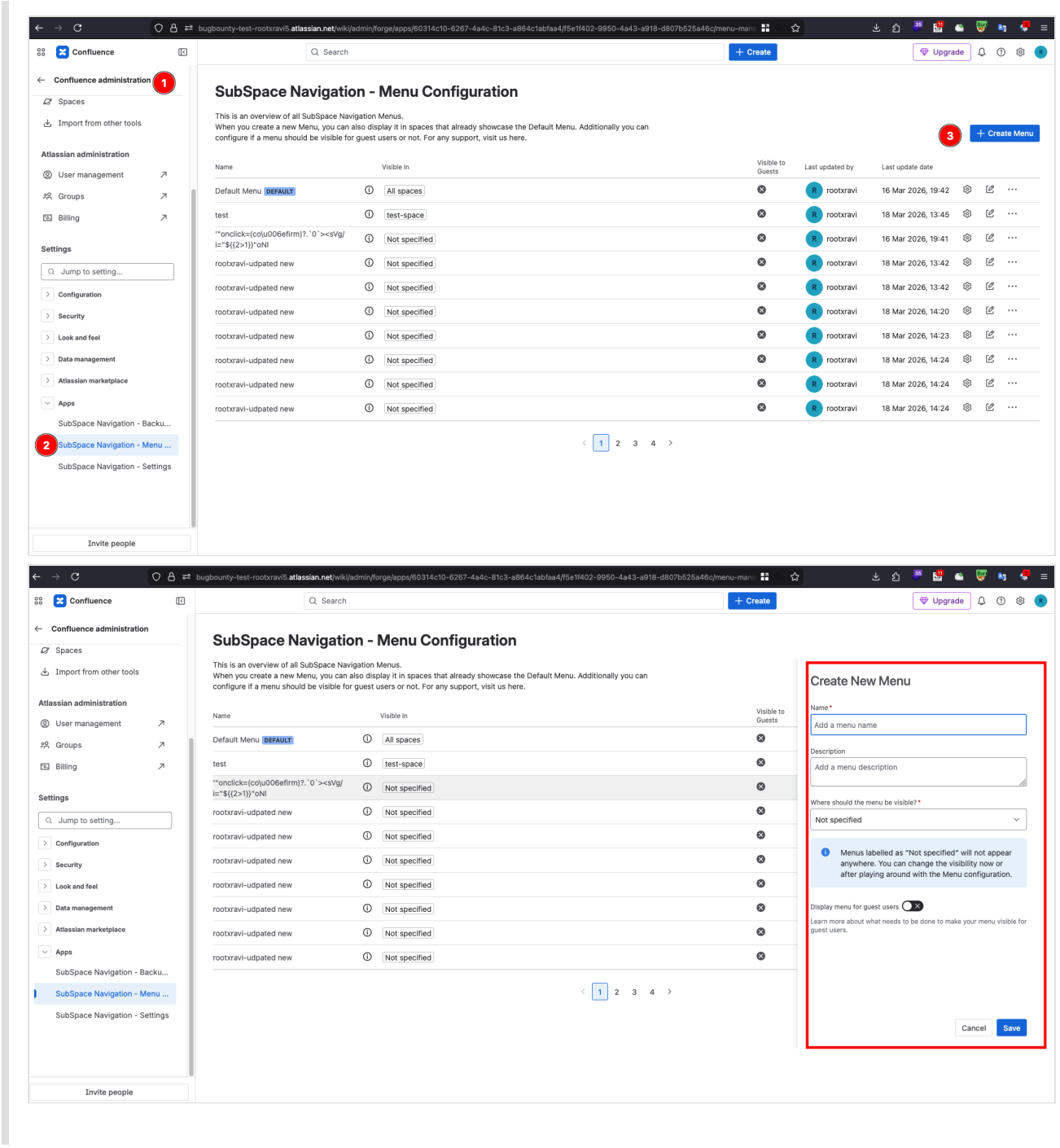
No rate limiting on a form can result in reputational damage to the organization if the rate limiting prevents legitimate form submissions and responses. It also has the potential to cause accelerated service usage, which can incur a direct financial cost in environments with SaaS services or pay on demand systems.

Steps to Reproduce

1. Create a Confluence instance and install the SubSpace Navigation for Confluence plugin using the following link:

   > https://marketplace.atlassian.com/apps/194/subspace-navigation-for-confluence?hosting=cloud&tab=overview

2. Navigate to the Confluence administration → Settings → Apps → SubSpace Navigation - Menu Configuration → Create menu



3. Fill out the form and submit the form while using the HTTP intercept proxy to intercept the request
4. Using the HTTP intercept proxy, re-issue the captured request 50 times in rapid succession
5. Observe within the HTTP intercept proxy that all 50 of these requests generate an ‘HTTP 200 OK’ response, showing that there is no rate-limiting on the form
6. Perform another, manual form submission in the browser
7. Observe that the form is submitted successfully which shows that there is no silent lockout implemented

```
POST /gateway/api/graphql?q=forge_ui_invokeExtension HTTP/2
Host: bugbounty-test-rootxravi5.atlassian.net
Cookie: ajs_anonymous_id=%2293474be7-0750-46e7-9b2d-a6f06e284bbf%22;
intercom-id-euzqi75u=089ad59d-262c-401f-85e5-7d47e14e2716; intercom-device-
id-euzqi75u=3c243b25-0cdd-4b72-9715-60089e55d0a0;
tenant.session.token=eyJraWQiOiJzZXNzaW9uLXNlcnZpY2UvcHJvZC0xNzM4Nzk0ODc0Iiw
iYWxnIjoiUlMyNTYifQ.eyJhc3NvY2lhdGlvbnMiOltdLCJzdWIiOiI3MTIwMjA6MDUwNzM2MTct
ZDQzYS00MDgxLTk2YmYtNTQyY2M0ZTVjNjQ1IiwiZW1haWxEb21haW4iOiJidWdjcm93ZG5pbmph
LmNvbSIsImltcGVyc29uYXRpb24iOltdLCJjcmVhdGVkIjoxNzczMTY4NTIxLCJyZWZyZXNoVGlt
ZW91dCI6MTc3MzgyMjA4NiwidmVyaWZpZWQiOnRydWUsImlzcyI6InNlc3Npb24tc2VydmljZSIs
InNlc3Npb25JZCI6IjNhM2VlN2ZiLTI3YTMtNGRjYy1hZjM0LTEzODI1ZTEwYWI5NiIsInN0ZXBV
cHMiOltdLCJhdWQiOiJhdGxhc3NpYW4iLCJuYmYiOjE3NzM4MjE0ODYsImV4cCI6MTc3NjQxMzQ4
NiwiaWF0IjoxNzczODIxNDg2LCJlbWFpbCI6InJvb3R4cmF2aSthZG1pbnJvb3R4cmF2aTVAYnVn
Y3Jvd2RuaW5qYS5jb20iLCJqdGkiOiIzYTNlZTdmYi0yN2EzLTRkY2MtYWYzNC0xMzgyNWUxMGFi
OTYifQ.TCS1vI-i0fzDPHdYaTrftXXxoxpxrY_dYCzSpG81HTJSHRsfJ0w79DM7TbNDe-
5qHocIX3ZZqZaOj5NtsbcA9wTSO3IwNd3pnw4VzXWyrx8XIYPRh7kM4c-
XIWAbjlhjgm4AAtkWdPfndcHDGz8hIOcf82MUieWI8UgQgaVtPmeBUSst5LCKp0afarRhwuxxPMQ
qFt7UhbbYW_8Z_Q7Bbcgjz1aEXMlGbeKQmHE37Y1k30OZdnYqdOA1SUZr8E5m-IJyx-
CcWb3_hOMsFmMzTb6TY__UFoAhPkDfjYjFcXz-ZNKoOd0YZRN18CvJwne0Gc-
AC2eIBeRupg594AoDDg; marketplace-launch-
darkly=%7B%22userKey%22%3A%220edf44d2-48f6-417c-9503-
35d6dbd89dd3%22%2C%22aaid%22%3A%22712020%3A05073617-d43a-4081-96bf-
542cc4e5c645%22%7D; jira_theme=dark; __awc_tld_test__=tld_test;
atlassian.account.xsrf.token=5acb621f-6304-4c61-b907-b58e05b99ec3; atl-
sticky-version={"currentVersion":"mrjf-prod-
18906","currentVersionExpiry":"1773762306146"};
atlassian.xsrf.token=a8fdf5e999028d23176705fe5b1ca47e635aee93_lin;
cb_nin=1|1|0|2; atl-bsc-consent-token-fallback=0031111010;
AWSALB=mfRICP0NgPDmW56Z97smhZebOkuQL2wsbCX/vxn0r2tkGbk7ZZ+E3jzPystdnhZ0PXNmO
D2/izOnsColodFBxqlWDoK+oIpuz2pMe1c57h1j41R9QnndHExNmqVa;
AWSALBCORS=mfRICP0NgPDmW56Z97smhZebOkuQL2wsbCX/vxn0r2tkGbk7ZZ+E3jzPystdnhZ0P
XNmOD2/izOnsColodFBxqlWDoK+oIpuz2pMe1c57h1j41R9QnndHExNmqVa;
io=Wyf1r8HpVjmsQfnBAJRz;
AWSALBTG=mCr1GNZ9pb4UcRGsBNEVr4I6/JCLJGic2qVI0B9WkKlH7oeEXh3xzst+jtMNxe/7I3Q
3RPHawnWqaEuzIMdZv8Q7LuB7qAFWmYDnsVaALpuXhXrr8fxE7WD4269RxF77j67u3HBv+14fE6B
NNlhVxENY1OYPibJvN9bNN56NAKgB;
AWSALBTGCORS=mCr1GNZ9pb4UcRGsBNEVr4I6/JCLJGic2qVI0B9WkKlH7oeEXh3xzst+jtMNxe/
7I3Q3RPHawnWqaEuzIMdZv8Q7LuB7qAFWmYDnsVaALpuXhXrr8fxE7WD4269RxF77j67u3HBv+14
fE6BNNlhVxENY1OYPibJvN9bNN56NAKgB;
JSESSIONID=LMIaDfABJqSkFUEqYSiFZ39W_zbF4JpFTtZs2HZd; atl-bsc-consent-
token=0031111010; atl-bsc-show-banner=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:148.0)
Gecko/20100101 Firefox/148.0
Accept: */*
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
```

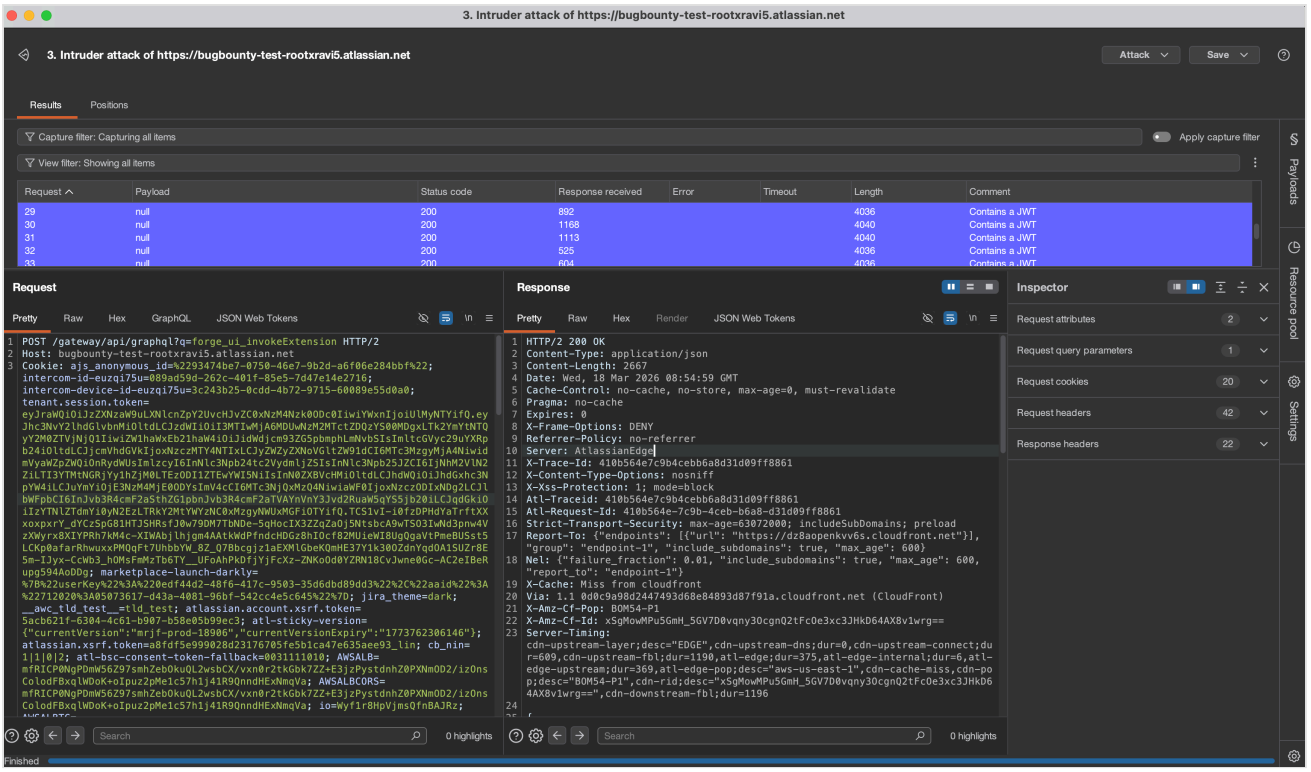
```
Referer: https://bugbounty-test-
rootxravi5.atlassian.net/wiki/admin/forge/apps/60314c10-6267-4a4c-81c3-
a864c1abfaa4/f5e1f402-9950-4a43-a918-d807b525a46c/menu-management
Content-Type: application/json
Atl-Attribution: {"product":"Confluence Cloud","service":"confluence-
frontend"}
X-Apollo-Operation-Name: forge_ui_invokeExtension
Atl-Edge-Region-Hint: prod-east
Atl-Agg-Confluence-Mutationerror-Compat: false
Content-Length: 3615
Origin: https://bugbounty-test-rootxravi5.atlassian.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers

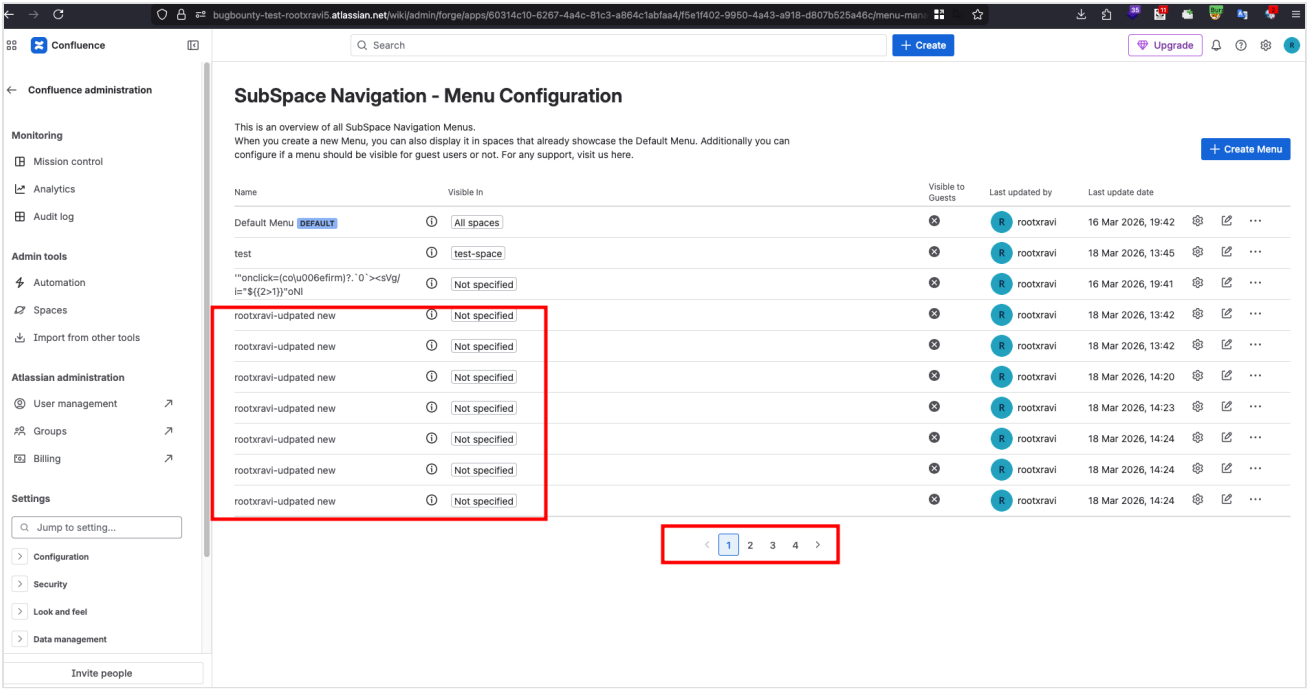
{"operationName":"forge_ui_invokeExtension","variables":{"input":
{"contextIds":["ari:cloud:confluence:bd6cb4b9-8047-4bf3-91f2-
410647436b14:workspace/88ab0bff-25a8-4a43-ae43-
cae7e3a4ed84"],"extensionId":"ari:cloud:ecosystem::extension/60314c10-6267-
4a4c-81c3-a864c1abfaa4/f5e1f402-9950-4a43-a918-d807b525a46c/static/menu-
management","payload":{"call":{"functionKey":"createMenu","payload":
{"name":"rootxravi-udpated new","description":"rootxravi-udpated
new","spaceKeys":[],"visibleToGuests":false}},"context":
{"cloudId":"bd6cb4b9-8047-4bf3-91f2-410647436b14","localId":"ari-cloud-
ecosystem--extension-60314c10-6267-4a4c-81c3-a864c1abfaa4-f5e1f402-9950-
4a43-a918-d807b525a46c-static-menu-management","environmentId":"f5e1f402-
9950-4a43-a918-
d807b525a46c","environmentType":"PRODUCTION","moduleKey":"menu-
management","siteUrl":"https://bugbounty-test-
rootxravi5.atlassian.net","appVersion":"3.0.0","extension":
{"type":"confluence:globalSettings"}},"contextToken":"eyJhbGciOiJSUzI1NiIsIm
tpZCI6ImZvcmdlL2NvbnRleHQtdG9rZW4vd2YtMzQ2YjVkNWItMzNmYi00NGRkLWJkZmYtMTQ2YT
VhMTk5MmZkIn0.eyJhY2NvdW50SWQiOiI3MTIwMjA6MDUwNzM2MTctZDQzYS00MDgxLTk2YmYtNT
QyY2M0ZTVjNjQ1IiwiYXBwSWQiOiJhcmk6Y2xvdWQ6ZWNvc3lzdGVtOjphcHAvNjAzMTRjMTAtNj
I2Ny00YTRjLTgxYzMtYTg2NGMxYWJmYWE0IiwiYXBwVmVyc2lvbiI6IjMuMC4wIiwiY29udGV4dC
I6eyJhY2NvdW50SWQiOiI3MTIwMjA6MDUwNzM2MTctZDQzYS00MDgxLTk2YmYtNTQyY2M0ZTVjNj
Q1IiwibG9jYWxlZCI6ImFyaS1jbG91ZC1lY29zeXN0ZW0tLWV4dGVuc2lvbi02MDMxNGMxMC02Mj
Y3LTRhNGMtODFjMy1hODY0YzFhYmZhYTQtZjVlMWY0MDItOTk1MC00YTQzLWE5MTgtZDgwN2I1Mj
VhNDZjLXN0YXRpYy1tZW51LW1hbmFnZW1lbnQiLCJjbG91ZElkIjoiYmQ2Y2I0YjktODA0Ny00Ym
YzLTkxZjItNDEwNjQ3NDM2YjE0IiwibW9kdWxlS2V5IjoibWVudS1tYW5hZ2VtZW50IiwiZW52aX
Jvbm1lbnRJZCI6ImY1ZTFmNDAyLTk5NTAtNGE0My1hOTE4LWQ4MDdiNTI1YTQ2YyIsImVudmlyb2
5tZW50VHlwZSI6IlBST0RVQ1RJT04iLCJzaXRlVXJsIjoiaHR0cHM6Ly9idWdib3VudHktdGVzdC
1yb290eHJhdmk1LmF0bGFzc2lhbi5uZXQiLCJhcHBWZXJzaW9uIjoiMy4wLjAiLCJleHRlbnNpb2
4iOnsidHlwZSI6ImNvbmZsdWVuY2U6Z2xvYmFsU2V0dGluZ3MifX0sImNvbnRleHRJZHMiOlsiYX
JpOmNsb3VkOmNvbmZsdWVuY2U6YmQ2Y2I0YjktODA0Ny00YmYzLTkxZjItNDEwNjQ3NDM2YjE0On
```

```
dvcmtzcGFjZS84OGFiMGJmZi0yNWE4LTRhNDMtYWU0My1jYWU3ZTNhNGVkODQiXSwiZXh0ZW5zaW
9uSWQiOiJhcmk6Y2xvdWQ6ZWNvc3lzdGVtOjpleHRlbnNpb24vNjAzMTRjMTAtNjI2Ny00YTRjLT
gxYzMtYTg2NGMxYWJmYWE0L2Y1ZTFmNDAyLTk5NTAtNGE0My1hOTE4LWQ4MDdiNTI1YTQ2Yy9zdG
F0aWMvbWVudS1tYW5hZ2VtZW50IiwidW5saWNlbnNlZCI6ZmFsc2UsImV4dGVuc2lvblR5cGUiOi
Jjb25mbHVlbmNlOmdsb2JhbFNldHRpbmdzIiwiaW5zdGFsbGF0aW9uSWQiOiJhNjk2ZDBiYS04MT
M3LTQyNjEtYTRlNC02YWViZTY0YzE2OGQiLCJpc3MiOiJmb3JnZS9jb250ZXh0LXRva2VuIiwiYX
VkIjoiZm9yZ2UiLCJpYXQiOjE3NzM4MjEzNzIsIm5iZiI6MTc3MzgyMTM3MiwiZXhwIjoxNzczOD
IyMjcyLCJqdGkiOiJmNTRmY2Y0NTE1OGQyZGQxZjBlZWQ5YjUzZTE4OWIxNGM1YWM4M2U4In0.Oh
WNPIwLg44dKB7XY-9R_cTfrJ3nOZ2zH3qXe8-ZOiWN6Uv3-2NW4hV3ctHsnT3G5OF4X-
CPmtwm_B-kF6WIMCgEbuB-
vhypMekq0Z5KsqRWXpM_KhWgkD6BwenGLvBWI0jYt6mpIqRDS_GajmgSIVSvMw21yNO9dfy298Yz
0bYHJKceTpcixffGdmjq4d_A5qX5Y7d3QfeykXe_NUp-AN_Hndo-
wW4559XmL9KVaiKfrxiAj4hwpBzSjrGyCHsf0eJoZEjc8zi2MzVvGinxy2PcpRLVRGWUygmmxD5d
aUZ-SaYf-4lOqr8DZxGG2lPeaxzdru8-
LVRfDowFkiwDZQ"},"entryPoint":"resolver"}},"query":"mutation
forge_ui_invokeExtension($input: InvokeExtensionInput!) {\n
invokeExtension(input: $input) {\n    success\n    response {\n      body\n
__typename\n    }\n    contextToken {\n      jwt\n      expiresAt\n
__typename\n    }\n    errors {\n      message\n      extensions {\n
errorType\n        statusCode\n        ... on
InvokeExtensionPayloadErrorExtension {\n          fields {\n
authInfoUrl\n            __typename\n          }\n          __typename\n
}\n        __typename\n      }\n      __typename\n    }\n    __typename\n
}\n}\n"}
```


Proof of Concept

The screenshot(s) below demonstrate(s) the vulnerability:





Target

https://marketplace.atlassian.com/apps/194/subspace-navigation-for-confluence?hosting=cloud&tab=overview

Vulnerability Rating Taxonomy (VRT)

Server Security Misconfiguration > No Rate Limiting on Form

Submission ID

be771d23-169f-42a3-9c79-9e4d8049663e

Reporting and Methodology

By leading with a best-in-class testing approach, Bugcrowd's methodology provides enhanced risk reduction while supporting critical compliance initiatives. A review of these standards follows.

Reviewed Organizational Methodology Standards:

- PCI DSS Requirement 11.2, 11.3.1, 11.3.3, 11.3.4
- NIST 800-115 - Technical Guide to Information Security Testing and Assessment 2.1 "Information Security Assessment Methodology"
- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)

In order to create a complete testing methodology, Bugcrowd has pulled from the following industry standard operational methodologies:

- OWASP Testing Guide (OTG)
- Web Application Hacker Handbook Methodology (WAHHM)
- Others where applicable (SANS Top 25, CREST, WASC, PTES)

Appendix A - Risk and priority key

The following key is used to explain how Bugcrowd rates valid vulnerability submissions and their technical severity. As a trusted advisor Bugcrowd also provides common "next steps" for program owners per severity category.

Technical severity	Example vulnerability types
P1 **Critical** Critical severity submissions (also known as "P1" or "Priority 1") are submissions that are escalated to Bugcrowd as soon as they are validated. These issues warrant the highest security consideration and should be addressed immediately. Commonly, submissions marked as Critical can cause financial theft, unavailability of services, large-scale account compromise, etc.	• Remote Code Execution • Vertical Authentication Bypass • XML External Entities Injection • SQL Injection • Insecure Direct Object Reference for a critical function
P2 **Severe** Severe severity submissions (also known as "P2" or "Priority 2") are vulnerability submissions that should be slated for fix in the very near future. These issues still warrant prudent consideration but are often not availability or "breach level" submissions. Commonly, submissions marked as Severe can cause account compromise (with user interaction), sensitive information leakage, etc.	• Lateral authentication bypass • Stored Cross-Site Scripting • Cross-Site Request Forgery for a critical function • Insecure Direct Object Reference for an important function • Internal Server-Side Request Forgery
P3 **Moderate** Moderate severity submissions (also known as "P3" or "Priority 3") are vulnerability submissions that should be slated for fix in the major release cycle. These vulnerabilities can commonly impact single users but require user interaction to trigger or only disclose moderately sensitive information.	• Reflected Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an important function • Insecure Direct Object Reference for an unimportant function
P4 **Low** Low severity submissions (also known as "P4" or "Priority 4") are vulnerability submissions that should be considered for fix within the next six months. These vulnerabilities represent the least danger to confidentiality, integrity, and availability.	• Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an unimportant function • External Server-Side Request Forgery
P5 **Informational** Informational submissions (also known as "P5" or "Priority 5") are vulnerability submissions that are valid but out-of-scope or are "won't fix" issues, such as best practices.	• Lack of code obfuscation • Autocomplete enabled • Non-exploitable SSL issues

VRT

Bugcrowd's Vulnerability Rating Taxonomy

More detailed information regarding our vulnerability classification can be found at: https://bugcrowd.com/vrt (https://bugcrowd.com/vrt)

Appendix B - Vulnerability details

This section outlines the full submission data for each valid finding. These findings are unaltered from their original state from the researcher. Due to the competitive nature and gamification of crowd-sourced security assessments, some typos or grammar errors may occur. Each finding is headlined with the submission title and priority followed by more detailed vulnerability information based on the type of finding submitted. Several other fields may appear based on the context and VRT classification selected by a researcher.

Such details may include the following:

Title

A brief summary of the vulnerability.

Bug URL

This is the full URL/URI of where the vulnerability took place

Description

This section appears above the "Reference Number" as a free form area for the researcher to describe the context of the submission. The full HTTP(S) request that triggered the vulnerability is normally in this field, including all its associated headers and cookie information.

Target

The target that is vulnerable.

Remediation advice

Steps to mitigate or compensate for the vulnerability.

Vulnerability Rating Taxonomy (VRT)

The Vulnerability Rating Taxonomy (https://bugcrowd.com/vrt) is the baseline guide used for classifying technical severity.

Jira ID

This is the ID to a customer Jira ticket associated with a vulnerability submission.

Custom fields

Some customers add extra attributes to vulnerability submissions, for example, "Product Start Version" or "Product End Version".

Submission ID

Submission ID is visible to customers and researchers.

bugcrowd

Bugcrowd Inc.
300 California St
Suite 220
San Francisco, CA 94104
(888)361-9734

23 Mar 2026

Closing Statement

Introduction

This report reflects testing of the Communardo assets targets between the dates of **February 11th, 2026** to **March 19th, 2026** . The purpose of this assessment was to identify security issues that could adversely affect the integrity of Communardo. The assessment was performed under the guidelines provided in the statement of work between Communardo and Bugcrowd. This document provides a high-level overview of the testing performed and the test results.

Pen Test Portfolio Overview

Our suite of Pen Test Products are powered by the Bugcrowd Platform, enabling rapid setup, launch, and real-time results.

While Bugcrowd offers both continuous and on-demand penetration testing options, it is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This document contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

Testing Methods

This security assessment leveraged researchers that used a combination of proprietary, public, automated, and manual test techniques throughout the assessment. Commonly tested vulnerabilities include code injection, cross-site request forgery, cross-site scripting, insecure storage of sensitive data, authorization/authentication vulnerabilities, business logic vulnerabilities, and more.

Summary of Findings

The summary of Bugcrowd's findings are as follows:

Severity	Number of findings
Critical	0
Severe	0
Moderate	0
Low	0
Informational	1