Acme Inc.

Bugcrowd Standard Pen Test (SPT)
Acme Inc. Infrastructure Network

Created On
March 01, 2023
Prepared By
Advanced Security Group (ASG)
Reviewed By
Advanced Security Group (ASG)

Contents

Executive Summary

Acme Inc., based in San Francisco, California, is a large importer/exporter of numerous products. As a requirement of their business, Acme Inc. maintains their infrastructure network that is responsible for gathering, transferring and storing all types of data. Acme Inc. has a requirement and obligation to ensure that this application is resilient to cyber-attack in order to protect the privacy of their customers. To assist with this, Acme Inc. employed Bugcrowd to perform a Standard Pen Test (SPT) which took place from February 20, 2023, through February 25, 2023.

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

To perform this test, our researcher leveraged several common tools to help identify and exploit vulnerable findings in the environment.

Manual testing of the scope was performed, evaluating the assets for weaknesses as per the Bugcrowd methodology. In support of this, active scanners and scripts were used in an attempt to identify any commonly found, known vulnerabilities.

At the time of this report, 6 findings were identified, including 1 Critical, 1 High, 1 Medium, 1 Low and 2 Informational vulnerabilities.

The highest priority vulnerabilities include:

- Sensitive Data Exposure where sensitive API keys and passwords were present in the internal GitHub Enterprise repositories.
- Sensitive Data Exposure where RPC ports were identified which disclosed further information about services which are running on the systems internally.

Bugcrowd has rated the overall risk to Acme Inc. – Infrastructure Network as Critical based on the Sensitive Data Exposures. Our rating is based on the severity of the findings disclosed within this report.

It is recommended that Acme Inc. focus on critical and high severity issues first, with medium, low and informational findings being fixed once all high and critical issues are remediated.

Bugcrowd recommends that all critical, high and medium 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 regular secure development training to developers to ensure that they are aware of secure development practices and emerging threats.

The continuation of this document contains technical details of the specific vulnerabilities that were discovered throughout the PTS engagement. It should be noted that many of the details, including comments, up-to-date remediation status, images and additional contexts are not present in this document and are only available in the Bugcrowd Customer Portal.

If you have any questions or concerns as you move to remediate the items raised in this report, please do not hesitate to contact us. Bugcrowd would like to thank Acme Inc. for this engagement and look forward to working together in the future.

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 program's findings (comments, code, and any researcher provided remediation information) can be found in the Bugcrowd Crowdcontrol platform.

Reporting and Methodology

Bugcrowd Standard Pen Test (SPT) is an on-demand methodology-driven penetration test that delivers real-time results and 24/7 reporting in support of a variety of compliance initiatives. A pay-per-project model powered by CrowdMatch technology enables Bugcrowd to draw from a global network of continuously vetted pentesters to deliver faster setup without compromising on skill or experience. To support accelerated remediation and streamline integrated business processes, vulnerabilities discovered during the methodology are viewable live in the Bugcrowd Customer Console as soon as they are submitted by the pentester. Bugcrowd's in-house team of Security Engineers works in parallel to validate, prioritize, and push streaming vulnerabilities through customer-chosen SDLC integrations like GitHub, JIRA, or ServiceNow.

The Bugcrowd Pen Test service was designed and independently assessed by a leading QSA to ensure alignment with key compliance and regulatory standards.

Our unique BugHunter testing methodology blends key organizational and operational elements of leading industry standards to create a unified methodology that satisfies auditor and reviewer requirements.

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

Organizational Methodology Standards

Executing a penetration test involves a proven workflow that is split into phases. Each of these phases is run in a cyclical manner allowing penetration testers to build upon findings and potentially uncover significant risk. An organizational methodology also ensures that high-level coverage of testing is done. When reviewing common organizational methodologies, Bugcrowd found similarities in the general workflow.

Bugcrowd pen testers adhere to these standards in a common workflow as shown:

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)

Operational Methodology Standards

Many penetration testing models fail to provide both results and coverage. To bring value to the customer, Bugcrowd has reviewed the most common and in-depth operational Pen Test methodologies. Operational methodologies provide details on what exactly needs to be tested in a security assessment, for each endpoint.

The methodology assigned to researchers includes application and infrastructure level testing domains. Each domain contains several tests for the tester to cover in both manual and automated methods.

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)

Findings Summary

Targets and Scope

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

The following targets were considered explicitly in scope for testing:

- Office External-Facing IPs
    - 66.244.216.12/28, 204.111.226.96/27 – Ottawa
    - 5.149.168.24/30, 217.173.115.104/29 – Dublin
    - 104.220.242.108/28, 65.222.195.0/28 – San Mateo
- General Subnet
    - 10.52.0.0/16, 10.234.0.0/16, 10.42.0.0/16 – Data Engineering
    - 10.224.0.0/12 – Corp Internal
    - 10.192.0.0/16 – Corp AWS
    - 10.200.0.0/22 – Corp Azure
    - 10.40.0.0/16 – AWS CA-CENTRAL Prod/MT
- External Targets
    - Truncated for Display
- Internal Targets
    - Truncated for Display

The following items are explicitly out-of-scope:

10.230.20.182	10.230.20.201	10.230.20.211	10.230.20.220
10.230.20.183	10.230.20.202	10.230.20.212	10.230.20.221
10.230.20.185	10.230.20.204	10.230.20.214	10.230.20.222
10.230.20.186	10.230.20.205	10.230.20.215	10.230.20.224
10.230.20.187	10.230.20.206	10.230.20.216	10.230.20.226
10.230.20.188	10.230.20.207	10.230.20.217	10.230.20.231
10.230.20.20	10.230.20.208	10.230.20.218	

All details of the program scope and full program brief are available in the Program Brief found on the Bugcrowd Crowdcontrol platform.

Risk and Priority Key

The following priority keys are used to explain how Bugcrowd rates valid vulnerability submissions and their technical severity. As a trusted advisor, Bugcrowd provides common next steps for program owners per severity category.

Priority	Technical Severity	Example Vulnerability Types
P1	Critical Severity vulnerabilities are escalated as soon as they are validated. These issues warrant the highest security consideration and should be addressed immediately.	• Remote Code Execution • Vertical Authentication Bypass • SQL Injection • Insecure Direct Object Reference for a critical function
P2	High Severity vulnerabilities should be slated for a fix very soon. These issues still warrant prudent consideration but are often not availability or "breach level" submissions.	• Lateral Authentication Bypass • Stored Cross-Site Scripting • Cross-Site Request Forgery for a critical function • Insecure Direct Object Reference for an important function
P3	Medium Severity vulnerabilities should be slated for remediation in a major release cycle.	• Reflected Cross-Site Scripting • Cross-Site Request Forgery for an important function • Insecure Direct Object Reference for an unimportant function
P4	Low Severity vulnerabilities should be considered for remediation within the next six months.	• Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an unimportant function • External Server-Side Request Forgery
P5	Informational findings are environmental information, best practices or potential accepted business risk.	• All open ports • Lack of Code Obfuscation • Autocomplete enabled • Non-exploitable SSL issues

Findings Table

Index	Title	VRT	Priority
F001	Hard-coded Passwords/API Keys in GitHub Repository	Sensitive Data Exposure	P1
F002	No Session Invalidation on Password Reset	Broken Authentication and Session Management	P2
F003	Information Disclosure – RPC Ports	Sensitive Data Exposure	P3
F004	Information Disclosure – Remote Desktop Protocol (RDP)	Sensitive Data Exposure	P4
F005	Lack of Security Headers	Server Security Misconfiguration	P5
F006	Old Version of Splunk Deployed	Using Components with Known Vulnerabilities	P5

Vulnerability Details

This section outlines the full submission data for each valid finding. These findings are rarely altered from their original state from the researcher. Due to the nature 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 Vulnerability Rating Taxonomy (VRT) classification selected by a researcher.

The details may include the following:

Description

This section appears after the "Bug URL" as a free form area for the researcher to describe the context of the submission.

Bug URL

This is the specific URL path or IP target location where the vulnerability was found.

Submission Reference Number

The unique identifier for the submission visible to researchers.

CVSS Rating

The CVSS vector string for this submission, if provided, and the score calculated from that vector string.

Vulnerability Rating Taxonomy (VRT)

The Vulnerability Rating Taxonomy is the baseline guide used for classifying technical severity.

Additional Details

Several other fields may appear based on the context and VRT classification selected by a researcher, such as but not limited to Bugcrowd Application Security Engineer (ASE) curated proof of concepts, comments to the researcher or Bugcrowd, assignees, attachments, and state change metadata. These can be viewed in the Crowdcontrol platform.

F001 - Hard-coded Passwords/API Keys in GitHub Repository

P1

Submission Reference Number
Dc61db1253b1a6887c52fb923c58923c81d602f10fc272a8ddb

Vulnerability Rating Taxonomy (VRT)
Sensitive Data Exposure > Disclosure of Secrets > For Internal Asset

Bug URL
https://code.corp.orderacme.com

Description
Disclosure of secrets for internal assets occurs when sensitive data for the internal assets is not behind an authorization barrier. When this information is exposed, it can place sensitive data, such as secrets, at risk. This can occur due to a variety of scenarios such as not encrypting data, secrets committed to GitHub within public repositories, or exposed internal assets.
Disclosure of secrets for this internal asset could be leveraged by an attacker to access the internal application or the environment where the application is hosted.

Business Impact:
Disclosure of secrets for internal assets can lead to indirect financial loss due to an attacker accessing, deleting, or modifying data from within the application. This could happen through an insider threat, existing data breaches, or a malicious internal attacker escalating their privileges. Reputational damage for the business can also occur via the impact to customers' trust that these events create. The severity of the impact to the business is dependent on the sensitivity of the data being stored in and transmitted by the application.

Steps to Reproduce:
1. Visit the IP: https://10.36.37.17/
2. Click the link of primary instance
3. Visit the following URLs and observe the response:

Finding Truncated for Display Purposes

F002 - No Session Invalidation on Password Reset

P2

Submission Reference Number
727992fe76d053e67d68fcaeb77fa88ec280b1190ee935ed

Vulnerability Rating Taxonomy (VRT)
Broken Authentication and Session Management > Failure to Invalidate Session > On Password Reset and/or Change

Bug URL
https://bugcrowd.com

Description

The session is not invalidated on password change.

Steps to Reproduce:

1. Login to: https://orderacme.com
2. In a new container window go to the same website again and click on forgot password within that login page
3. Check the link in the email and reset the password of that user
4. Go back to the logged-in user, reload the page or browse through normally, notice that the web app session does not invalidate on password change

Finding Truncated for Display Purposes

F003 - Information Disclosure - RPC Ports

P3

Reference Number
4e7b75cbf48b0ffcf89e5ba098b85e7c1b134c186afafc06a

VRT
Sensitive Data Exposure > Disclosure of Secrets > For Internal Asset

Bug URL
10.36.9.224

Description
RPC Port was discovered open on the following IPs:

- 10.36.9.224
- 10.36.164.26
- 10.36.252.153
- 10.36.368.70
- 10.224.1.18

Running the rpcinfo command disclosed further information about the services which are running on the systems internally.

Proof of Concept (PoC):

The screenshots below show the full output of the command:

Finding Truncated for Display Purposes

F004 - Information Disclosure – Remote Desktop Protocol (RDP)

P4

Submission Reference Number
dacba07473fe7c26e8dc6a626f7da6a79e5d9be31d07b61f

Vulnerability Rating Taxonomy (VRT)
Other

Bug URL
10.230.0.6

Vulnerability

It was observed that the RDP service running in the below-mentioned hosts disclose server information:

- 10.40.16.224
- 10.40.144.246
- 10.32.32.232
- 10.32.33.62
- 10.32.34.32
- 10.36.32.32

Steps to Reproduce:
The following nmap command was used to determine the information disclosed by the service:

```
nmap -Pn -sV --script rdp-ntlm-info -p 3389 -iL hosts.txt
```

Proof of Concept (PoC):
The following screenshot demonstrates the information being disclosed

Finding Truncated for Display Purposes

F005 - Lack of Security Headers

P5

Submission Reference Number
D773d2e03558533a3e4f7c4dd7d4335bbc4f07499eb8e5a18

Vulnerability Rating Taxonomy (VRT)
Other

Vulnerability

A lack of HTTP response security headers can lead to sensitive user data being retrieved by an attacker through Cross-Site Scripting (XSS), Man-in-the-Middle (MitM), clickjacking, and some local network attacks. There are multiple HTTP response headers used in communication between the server and client, which can be implemented to improve security against well documented vulnerabilities.

An advanced attacker can leverage a missing security headers to bypass security controls of an application to execute code within a user's browser or capture data in transit.

Steps to Reproduce:
1. Enable an HTTP interception proxy, such as Burp Suite or OWASP ZAP
2. Navigate to the following endpoint using a browser
3. Capture the request using the HTTP interception proxy and review the response
4. Observe that the security headers are not implemented according to best practice

Missing Headers and Affected URLs:
Strict-Transport-Security:
-
Content Security Policy (CSP):
-
X-Frame-Options:
-
X-Content-Type-Options:
-

Finding Truncated for Display Purposes

F006 - Old Version of Splunk Deployed

P5

Submission Reference Number
64ccefb37786297289bbca685df42ea86eb794a5d0e1982

Vulnerability Rating Taxonomy (VRT)
Using Components with Known Vulnerabilities > Outdated Software Version

Bug URL
10.32.168.39:8089

Description
It was observed that the version of splunkd service running on the following hosts is outdated.

The latest version of Splunk is 9.0.0.1:

- 10.32.163.32:8089
- 10.32.164.137:8089
- 10.32.165.39:8089

Proof of Concept (PoC):
The following screenshot demonstrates the version number of the service running:

Finding Truncated for Display Purposes

Closing Statement

Bugcrowd Inc.
921 Front Street
Suite 100
San Francisco, CA 94111

March 01, 2023

Summary

This report shows testing of Acme Inc. – Infrastructure Network from February 20, 2023, to February 25, 2023. The purpose of this assessment was to identify security issues that could adversely affect the integrity of Acme Inc. – Infrastructure Network. The assessment was performed under the guidelines provided in the statement of work between Acme Inc. and Bugcrowd. This document provides a high-level overview of the testing performed and the test results.

Pen Test Portfolio Overview

The Bugcrowd Pen Test portfolio provides organizations with the power of the Crowd, through two unique engagement styles designed to fit a range of security workflows and objectives. Max Pen Test (MPT), Plus Pen Test (PPT) and Standard Pen Test (SPT) are all 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.

The summary of Bugcrowd's findings are as follows:

1 Critical **1 High** **1 Medium** **1 Low** **2 Informational**