[ACME Logo]

SECURITY ASSESSMENT REPORT DRAFT TLP:AMBER

External Network
Penetration Testing

[Client Logo]

PREPARED EXCLUSIVELY FOR

Global Finance Corp

123 Financial District Blvd, Suite 400
New York, NY 10004

DATE OF ISSUANCE	REPORT PERIOD	REVISION	PREPARED BY
September 23, 2026	Q3 2026	Rev 1.1	ACME Offensive Security

[ACME Logo]

TABLE OF **CONTENTS**

[ACME Logo]

EXECUTIVE **SUMMARY**

Global Finance Corp's external network infrastructure serves as the digital gateway for critical financial operations and customer interactions.

The current assessment reveals a network perimeter characterized by established patch management and security implementations. Notable findings include specific unpatched web servers and minor misconfigurations within the DMZ environment.

Despite the identified vulnerabilities, the external infrastructure continues to reliably support business operations with no evidence of active exploitation or immediate critical compromise paths.

The assessment findings reveal opportunities to strengthen the external security posture through improvements in service configurations. The identified configuration gaps impact overall security maturity, resulting in the following security rating:

RISK RATING

SATISFACTORY
Security meets industry standards. Minimal to no actionable findings identified.

NEEDS IMPROVEMENT
Protects some areas, but moderate changes and configuration updates are required.

NON SATISFACTORY
Significant security deficiencies exist requiring immediate attention.

[ACME Logo]

CYBERSECURITY
MATURITY SCORE

EXECUTIVE TAKEAWAY

Your external network security is fundamentally sound, placing you in the upper "Average" tier. With targeted remediation, achieving a "Good" rating is highly attainable.

Global Finance Corp's external network cybersecurity maturity places the organization in the upper range of the Average tier relative to its enterprise-size peers, positioned just below the threshold of the Good tier. This reflects a security posture that is consistent with industry norms for organizations of comparable scale, while highlighting a clear opportunity for advancement. By addressing the findings identified in this assessment, Global Finance Corp is well-positioned to close the remaining gap, strengthening its resilience against external threats.

UNDERSTANDING THIS CHART

This chart compares cybersecurity maturity across varying company sizes, with the indicator dot marking your organization's exact position based on current assessment findings.

Maturity Scores by Company Size

2026 Assessment across organization sizes with Global Finance Corp positioning

[ACME Logo]

SCOPE & **METHODOLOGY**

SCOPE HIGHLIGHTS

- ✓ **Comprehensive mapping of internet-facing assets**
- ✓ **Passive and active reconnaissance techniques**
- ✓ **Coverage across Cloud, Transit, and Regional ISPs**

The external network penetration test encompassed Global Finance Corp's internet-facing infrastructure across several IP ranges supporting critical banking operations.

ACME Security employed advanced external reconnaissance techniques combining both passive and active discovery methods to identify all internet-accessible services and potentially hidden infrastructure components.

Our methodology included comprehensively reviewing public information sources, such as autonomous system registrations, to ensure complete coverage and mapping of all internet-facing assets prior to active vulnerability testing and exploitation phases.

External Network Infrastructure

Internet-facing assets across regional ISPs and distributed networks

[ACME Logo]

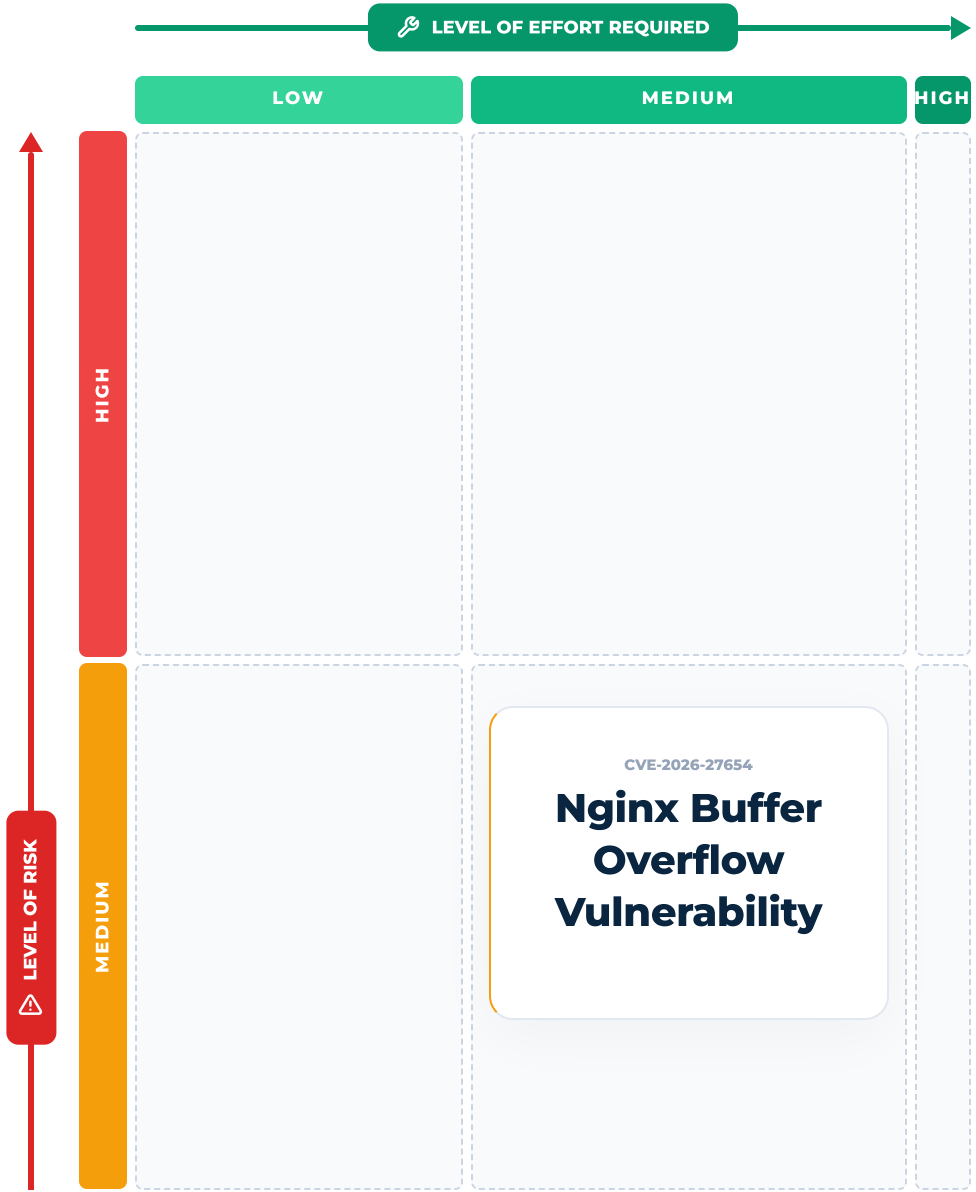
RISK **MATRIX**

PRIORITIZATION STRATEGY

Focus first on the top-left quadrant (High Risk, Low Effort) to eliminate critical vulnerabilities with minimal resource expenditure.

The following matrix shows a visual summary of recommendations mapped against two critical dimensions: the **Level of Risk** (severity of potential impact) and the **Level of Effort Required** (resources required to remediate) to mitigate the finding to an acceptable level.

ACME Consulting recommends utilizing this matrix to triage remediation efforts across your internal development and operations teams. By systematically addressing high-risk / low-effort tasks first, Global Finance Corp can immediately lower the volume of actionable findings to a more manageable level and maximize security ROI.



[ACME Logo]

TESTING **PHASES**

METHODOLOGY APPROACH

Our rigorous four-stage framework ensures comprehensive coverage, eliminates false positives, and delivers actionable, business-centric remediation strategies.

ACME Consulting performed the penetration testing using a proven, four-phase methodology. The primary purpose of this approach is to identify and validate as many business-critical vulnerabilities as possible within the defined scope of this engagement.

In addition to active exploitation, we collected all relevant vulnerabilities, meticulously eliminated false positives, and mapped the remaining findings to the corresponding information security controls currently implemented by the company. This allows us to accurately evaluate the real-world effectiveness of your preventative and detective defense mechanisms.

1

Intelligence Gathering

Gather as much information as possible to be utilized when penetrating the target during the active exploitation phases.

2

Threat Modeling

Identify, enumerate, and prioritize potential attack vectors and vulnerabilities entirely from an attacker's point of view.

3

Vulnerability Analysis

Discover flaws in systems, services, and applications which can be actively leveraged and exploited by an attacker.

4

Reporting

Document findings, provide remediation strategies, and deliver actionable recommendations to secure the environment.

[ACME Logo]

FINDINGS **OVERVIEW**

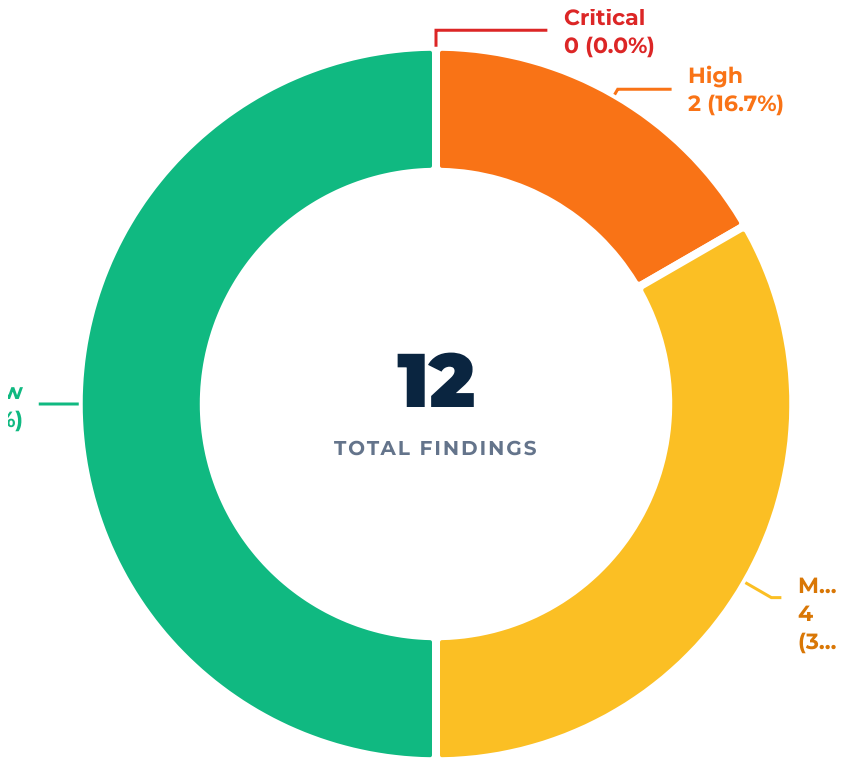
RISK ASSESSMENT CRITERIA

Vulnerabilities are rigorously scored based on internet exposure, potential business impact, likelihood of exploitation, and ease of external access.

The following section presents a comprehensive analysis of all security vulnerabilities identified during the external network penetration test. Each finding has been carefully evaluated and assigned a standardized risk rating to prioritize remediation efforts effectively across your internal teams.

The assessment successfully identified **12 distinct security findings** across Global Finance Corp's external network infrastructure. The chart to the right provides a high-level breakdown of these vulnerabilities by their assigned severity level, serving as a roadmap for immediate technical action.

Risk Rating Overview



0	2	4	6
CRITICAL	HIGH	MEDIUM	LOW

FINDING 1

Nginx Buffer Overflow Vulnerability (CVE-2026-27654)

RISK LEVEL

Medium

AFFECTED SECURITY CONTROL

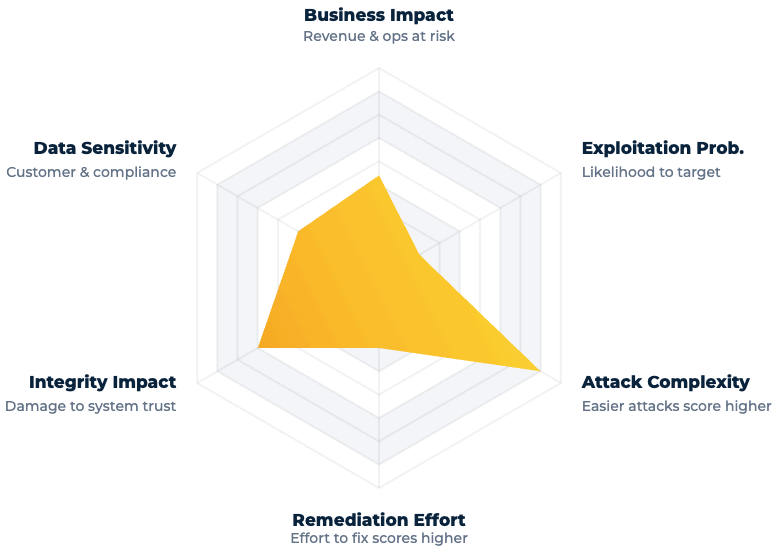
Remote Access Management

COMPLIANCE IMPACT

`NIST CSF: PR.AC-3`

TOTAL AFFECTED HOSTS

2



5.9

RISK SCORE

Affected Hosts

`181.119.220.213` `181.119.220.228`

Vulnerability Description

ACME Security identified a heap-based buffer overflow vulnerability affecting the `ngx_http_dav_module` in NGINX Open Source and NGINX Plus. This vulnerability allows remote attackers to trigger a buffer overflow in the NGINX worker process, potentially resulting in worker process termination (denial of service) or unauthorized modification of source and destination file names outside the document root.

The vulnerability is exploitable when specific configuration conditions are met: the NGINX configuration must use the DAV module's MOVE or COPY methods in combination with prefix location and alias directives. While the integrity impact is constrained, successful exploitation leads to service disruption.

Remediation & Solution Strategy

ACME Consulting recommends taking the following corrective actions in order of priority:

1. Apply Vendor Patches

Upgrade all affected NGINX instances to the latest stable release provided by F5/NGINX to address the CVE-2026-27654 advisory directly at the source.

2. Configuration Mitigation (If patching is delayed)

Temporarily mitigate the risk by modifying NGINX configurations. Disable the `ngx_http_dav_module` if it is not strictly required. If required, avoid using the `alias` directive in conjunction with DAV methods.

3. Web Application Firewall (WAF)

Ensure your perimeter WAF is configured to inspect and strictly validate the format and length of HTTP headers associated with WebDAV COPY and MOVE methods, blocking malformed requests.

PROOF OF **CONCEPT**

✕ EXPLOIT ATTEMPT UNSUCCESSFUL

This slide demonstrates ACME Consulting's attempt to actively exploit the identified vulnerability (CVE-2026-27654). While the server is running the vulnerable software version, environmental configurations actively prevented successful execution of the payload.

EVIDENCE 1: VERSION IDENTIFICATION

Network Headers - 181.119.220.213

▼ General	
Request URL	http://181.119.220.213/
Request Method	GET
Status Code	● 304 Not Modified
▼ Response Headers	
Connection	keep-alive
Date	Fri, 21 Aug 2026 21:24:27 GMT
Server	nginx/1.28.3
▼ Request Headers	
Accept	text/html,application/xhtml+xml,application/xml...
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...

EVIDENCE 2: ACTIVE EXPLOITATION ATTEMPT

acme@kali: ~/Desktop/Pentest

```
-(acme@kali)-[~/Desktop/Pentest]
$ python3 poc.py --target 181.119.220.213

CVE-2026-27654 -- nginx dav_module DAV alias path handling PoC

Target: http://181.119.220.213
Mode: crash
DAV: /uploads/

[*] Checking target connectivity ...
[+] Target is up

[*] PUT http://181.119.220.213/uploads/triggerfile.txt
[-] PUT failed (405): <html>
<head><title>405 Not Allowed</title></head>
<body>
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx</center>
[!] PUT failed. Check that the DAV location uses 'alias' +
'dav_methods'.
```

[ACME Logo]

ENGAGEMENT **TEAM**

The following security professionals were exclusively assigned to this engagement. Our team combines decades of offensive security experience, advanced exploit development, and enterprise risk management to deliver highly contextualized and actionable results.

Dr. Marcus Reed

LEAD PENETRATION TESTER

`OSCP` `OSCE` `CISSP`

Marcus brings over 12 years of experience in offensive security, specializing in external perimeter assessments and red team operations for global financial institutions. He leads the technical execution and vulnerability validation for ACME's most critical accounts.

Elena Rostova

SENIOR SECURITY CONSULTANT

`OSEP` `OSWE` `GXPN`

Elena is a recognized expert in advanced web application exploitation and evasive tradecraft. Her deep knowledge of modern frameworks and custom payload development ensures that even the most obscure logic flaws and bypasses are identified and mitigated.

David Chen

CLOUD SECURITY SPECIALIST

`AWS-SEC` `AZ-500` `CCSP`

David focuses exclusively on identifying misconfigurations and attack paths within distributed cloud environments. He mapped and analyzed the Azure and AWS components of the engagement, ensuring comprehensive coverage of the hybrid infrastructure.

Sarah Jenkins

ENGAGEMENT MANAGER

`CISM` `CISA` `PMP`

Sarah bridges the gap between highly technical findings and executive risk management. She coordinates the rules of engagement, oversees project delivery timelines, and ensures all reporting aligns with the strategic business objectives of the client.

[ACME Logo]

CAPABILITY **STATEMENT**

ACME Consulting has assembled a diverse and inclusive team of talented, hardworking professionals with more than 20 years of experience operating in the Information Security and Cybersecurity space. Our specialized offensive security team has achieved industry-leading certifications including CISSP, CISA, CRISC, CGEIT, OSCP, and CPM.

We are deeply committed to delivering high-quality services that consistently meet and exceed client expectations. We maintain rigorous quality control processes, adhere to industry best practices, and tailor our methodologies to fit the unique risk profile of every organization we engage with.

PAST PERFORMANCE

Private Entities

ACME Consulting has successfully completed highly sensitive engagements for clients across diverse, heavily regulated industries.

Client Logo

Client Logo

Client Logo

Client Logo

Client Logo

Client Logo

Dun & Bradstreet License Number

080568062

https://cage.report/DUNS/080568062

Public Entities

ACME is fully authorized to provide services to the US Federal Government. Below are select agencies and municipalities we have supported.

Agency Logo

Agency Logo

Agency Logo

Agency Logo

Approved Federal Commercial Entity (CAGE)

80A06

https://cage.dla.mil/Search/Details?id=10010813

[Large ACME Logo]

CORPORATE PROFILE

ACME Consulting

ACME Consulting is a premier offensive security and cyber risk advisory firm. For over two decades, we have partnered with highly regulated enterprises and federal agencies to identify, validate, and remediate complex vulnerabilities before they can be exploited by malicious actors. Our mission is to transform theoretical risk into actionable security.

GLOBAL HEADQUARTERS

ACME Consulting Group, LLC

One World Trade Center, Suite 4500
New York, NY 10007

CORE FOCUS	GENERAL INQUIRIES	EMAIL SUPPORT	WEBSITE
Offensive Security	**+1 (800) 555-ACME**	**engage@acmecyber.com**	**www.acmecyber.com**