SAMPLE REPORT - FOR DEMONSTRATION PURPOSES ONLY

ZIO SECURITY

Expert Security Testing

External Risk Review

ACME Corporation

Report Date: February 4, 2026

Assessment Period: January 28 - February 3, 2026

Version: 1.0

CONFIDENTIAL

Bottom Line: ACME Corporation' external security posture has several areas requiring attention. We identified 7 vulnerabilities across your public-facing infrastructure, including 1 critical and 2 high-severity issues that should be addressed within the next 7 days.

The most significant risks involve a missing DMARC policy that allows email spoofing, an outdated SSL/TLS configuration on your customer portal, and employee credentials found in public data breaches. These are exactly the types of weaknesses attackers look for when targeting organizations.

Good news: Your main website is properly configured with modern security headers, your DNS records show no signs of hijacking vulnerabilities, and your web application firewall is correctly blocking common attack patterns.

FINDINGS AT A GLANCE

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	2	2	1	1

KEY RECOMMENDATIONS

1. **Implement DMARC policy** — Prevents attackers from sending emails that appear to come from your domain. This protects customers and staff from phishing.
2. **Update SSL/TLS on customer portal** — Disable outdated TLS 1.0/1.1 protocols to protect customer data in transit.
3. **Force password resets for exposed accounts** — 3 employee credentials were found in breaches. Reset these immediately and enable MFA.

SCOPE

This assessment covered the external attack surface of ACME Corporation, including:

- **Primary Domain:** acme-corp.com
- **Subdomains:** portal.acme-corp.com, mail.acme-corp.com, vpn.acme-corp.com
- **IP Ranges:** 203.0.113.0/24
- **Email Domain:** acme-corp.com

TESTING METHODOLOGY

Our assessment followed industry-standard methodologies including OWASP, PTES, and NIST guidelines. Testing was conducted from an external perspective, simulating what an attacker could discover and exploit without internal access.

ASSESSMENT AREA	DESCRIPTION
Attack Surface Mapping	Discovery of all public-facing assets, DNS records, subdomains, and exposed services
Vulnerability Testing	Identification of known vulnerabilities in exposed services and applications
Email Security	Analysis of SPF, DKIM, and DMARC configurations
SSL/TLS Analysis	Certificate validation and cryptographic configuration review
Credential Exposure	Search for breached credentials associated with the organization
DNS Security	Zone configuration and DNS hijacking risk assessment

SAMPLE REPORT - FOR DEMONSTRATION PURPOSES ONLY

ID	FINDING	SEVERITY	CVSS	NIST CSF
ZIO-001	Remote Code Execution on Public Web Application	CRITICAL	9.8	PR.DS-2
ZIO-002	Breached Employee Credentials Discovered	HIGH	7.4	PR.DS-2
ZIO-003	Exposed Administrative Panel	HIGH	7.2	PR.AC-5
ZIO-004	Missing Rate Limiting on Authentication Endpoint	MEDIUM	5.3	PR.AC-5
ZIO-005	Missing Security Headers on Portal	MEDIUM	4.7	PR.IP-1
ZIO-006	SSL Certificate Expires in 21 Days	LOW	3.1	PR.DS-2
ZIO-007	Directory Listing Enabled on Dev Server	INFO	0.0	ID.AM-1

SEVERITY DEFINITIONS

SEVERITY	CVSS RANGE	DESCRIPTION
CRITICAL	9.0 - 10.0	Immediate exploitation likely; significant business impact. Remediate within 24-48 hours.
HIGH	7.0 - 8.9	Exploitation probable; major impact. Remediate within 7 days.
MEDIUM	4.0 - 6.9	Exploitation possible; moderate impact. Remediate within 30 days.
LOW	0.1 - 3.9	Exploitation unlikely; minor impact. Remediate within 90 days.
INFO	0.0	Informational finding; best practice recommendation.

SAMPLE REPORT - FOR DEMONSTRATION PURPOSES ONLY

Remote Code Execution on Public Web Application

ZIO-001

CRITICAL

CVSS SCORE	CVSS VECTOR	NIST CSF	AFFECTED ASSET
9.8	**AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**	PR.IP-1	**portal.acme-corp.com**

DESCRIPTION

We discovered a critical remote code execution vulnerability in the web application running on your customer portal. The application is running an outdated version of Apache Struts (2.3.x) that is vulnerable to CVE-2017-5638, allowing unauthenticated attackers to execute arbitrary commands on the server.

BUSINESS IMPACT

An attacker exploiting this vulnerability could:

- Gain complete control of the web server
- Access customer data stored in connected databases
- Use the compromised server as a pivot point to attack internal systems
- Install ransomware or other malware
- Cause significant business disruption and reputational damage

EVIDENCE

Vulnerability scan identified outdated Apache Struts version:

```
$ nuclei -u https://portal.acme-corp.com -t cves/2017/CVE-2017-5638.yaml [CVE-2017-5638] [critical]
https://portal.acme-corp.com Apache Struts 2.3.x RCE via Content-Type header
```

REMEDIATION

1. Immediately update Apache Struts to the latest version (2.5.x or newer)
2. If immediate patching is not possible, implement WAF rules to block exploitation attempts
3. Review server logs for signs of previous exploitation
4. Consider a full security assessment of the application after patching

REFERENCES

DMARC.org • HHS regulatory Cybersecurity Guidance

ZIO-002

HIGH

CVSS SCORE	CVSS VECTOR	NIST CSF	AFFECTED ASSET
7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	PR.DS-2	portal.acme-corp.com

DESCRIPTION

The customer portal accepts connections using TLS 1.0 and TLS 1.1, which are outdated protocols with known security vulnerabilities. These protocols are deprecated and no longer considered secure for protecting sensitive data in transit.

BUSINESS IMPACT

Attackers on the same network as a customer (such as public WiFi) could potentially intercept and decrypt sensitive business data transmitted to/from the portal. This is a regulatory compliance concern for protecting sensitive data in transit.

EVIDENCE

```
$ sslyze portal.acme-corp.com TLS 1.0: ENABLED (INSECURE) TLS 1.1: ENABLED (INSECURE) TLS 1.2: ENABLED TLS 1.3: ENABLED
```

REMEDIATION

1. Access your web server or load balancer configuration
2. Disable TLS 1.0 and TLS 1.1 protocols
3. Ensure TLS 1.2 and TLS 1.3 remain enabled
4. Test with SSLLabs.com to verify changes
5. Note: This may affect users on very old browsers (IE 10 and below)

Exposed Administrative Panel

ZIO-003

HIGH

CVSS SCORE	CVSS VECTOR	NIST CSF	AFFECTED ASSET
7.4	AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N	PR.AC-1	3 employee accounts

DESCRIPTION

These credentials were exposed in third-party breaches (not a breach of your systems) but pose a risk if employees reuse passwords across services.

BUSINESS IMPACT

If any of these employees use the same password for their work accounts, attackers could gain unauthorized access to your systems. This is especially concerning for organizations where such access could lead to sensitive data exposure.

EVIDENCE

EMAIL	BREACH SOURCE	DATE
j.smith@acme-corp.com	LinkedIn 2021	2021-06-22
m.johnson@acme-corp.com	Adobe 2019	2019-10-15
r.davis@acme-corp.com	Dropbox 2016	2016-08-31

Note: Actual passwords not displayed for security.

REMEDIATION

1. Force immediate password reset for the 3 affected accounts
2. Enable multi-factor authentication (MFA) on all accounts if not already enabled
3. Remind employees not to reuse passwords across personal and work accounts
4. Consider implementing a password manager for the organization

Missing Rate Limiting on Authentication Endpoint

ZIO-004

MEDIUM

CVSS SCORE	CVSS VECTOR	NIST CSF	AFFECTED ASSET
5.3	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	PR.AC-5	acme-corp.com/wp-admin

DESCRIPTION

The WordPress admin login page is publicly accessible at a predictable URL (/wp-admin). While this alone isn't a vulnerability, it makes it easier for attackers to find and target your login page with brute-force or credential stuffing attacks.

BUSINESS IMPACT

Exposed admin pages are frequently targeted by automated attack tools. Combined with the breached credentials finding, this increases the risk of unauthorized admin access.

REMEDIATION

1. Install a WordPress security plugin (Wordfence, Sucuri) to add login protection
2. Enable login attempt limiting (lock out after 5 failed attempts)
3. Consider restricting admin access to specific IP addresses
4. Ensure MFA is enabled for all admin accounts

Missing Security Headers on Portal

ZIO-005

MEDIUM

CVSS SCORE	CVSS VECTOR	NIST CSF	AFFECTED ASSET
4.7	AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N	PR.IP-1	portal.acme-corp.com

DESCRIPTION

The customer portal is missing several recommended HTTP security headers that help protect users from various web-based attacks.

EVIDENCE

HEADER	STATUS	PURPOSE

X-Frame-Options	Missing	Prevents clickjacking
X-Content-Type-Options	Present	Prevents MIME sniffing
Strict-Transport-Security	Missing	Forces HTTPS

REMEDIATION

Add the following headers to your web server configuration:

```
Content-Security-Policy: default-src 'self' X-Frame-Options: DENY Strict-Transport-Security: max-age=31536000; includeSubDomains
```

SSL Certificate Expires in 21 Days

ZIO-006

LOW

CVSS SCORE	NIST CSF	AFFECTED ASSET
3.1	PR.DS-2	vpn.acme-corp.com

DESCRIPTION

The SSL certificate for your VPN portal expires on February 25, 2026. If not renewed, users will see security warnings and may be unable to connect.

REMEDIATION

Renew the SSL certificate before expiration. Consider setting up auto-renewal with Let's Encrypt or configuring calendar reminders 30 days before future expirations.

Directory Listing Enabled on Dev Server

ZIO-007

INFO

CVSS SCORE	NIST CSF	AFFECTED ASSET
0.0	ID.AM-1	dev.acme-corp.com

DESCRIPTION

exposed, this server should not be publicly accessible.

REMEDIATION

Restrict access to development servers using IP allowlisting or VPN requirements. Disable directory listing in the web server configuration.

The following roadmap prioritizes remediation efforts based on risk severity and implementation complexity. We recommend addressing issues in the order presented.

PRIORITY	FINDING	EFFORT	TIMELINE
Immediate 24-48 hours	ZIO-001: Remote Code Execution	Low	Week 1
Immediate 24-48 hours	ZIO-002: Breached Credentials (force reset)	Low	Week 1
Short-term 1-7 days	ZIO-003: Exposed Admin Panel	Medium	Week 1-2
Medium-term 1-4 weeks	ZIO-004: Missing Rate Limiting	Low	Week 2-3
Medium-term 1-4 weeks	ZIO-005: Missing Security Headers	Medium	Week 2-4
Long-term 1-3 months	ZIO-006: SSL Certificate Renewal	Low	Before Feb 25
Long-term 1-3 months	ZIO-007: Dev Server Access	Low	Month 2

EFFORT DEFINITIONS

- **Low:** Configuration change, no development required (< 2 hours)
- **Medium:** Some development or coordination required (2-8 hours)
- **High:** Significant development or infrastructure changes (> 8 hours)

This External Risk Review identified 7 vulnerabilities in ACME Corporation' external attack surface. The most critical issues—the missing DMARC policy and breached credentials—can be addressed quickly and will significantly improve your security posture.

RECOMMENDED NEXT STEPS

1. **Address critical findings this week** — Implement DMARC and reset compromised passwords within the next 48 hours.
2. **Schedule TLS update** — Coordinate with your IT team to disable old TLS protocols on the customer portal during a maintenance window.
3. **Complete remaining items** — Use the roadmap above to work through medium and low priority items over the next 30-90 days.
4. **Verify fixes** — After remediation, we'll re-test to confirm vulnerabilities are resolved (included in your engagement).
5. **Ongoing monitoring** — Your 3-month monitoring subscription will alert you to new issues as they arise.

QUESTIONS?

If you have questions about any findings or need help prioritizing remediation, contact us at **support@ziosecurity.com**.

Thank you for choosing Zio Security.

The following tools were used during this assessment:

TOOL	PURPOSE
Nmap	Port scanning and service enumeration
Nuclei	Vulnerability scanning
SSLyze	SSL/TLS configuration analysis
Subfinder / Amass	Subdomain enumeration
Dehashed	Credential breach search
MXToolbox	Email security analysis
SecurityHeaders.com	HTTP header analysis

Findings in this report are mapped to the NIST Cybersecurity Framework (CSF) to support compliance and risk management efforts.

NIST CSF CONTROL	DESCRIPTION	RELATED FINDINGS
ID.AM-1	Physical devices and systems are inventoried	ZIO-007
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited	ZIO-003
PR.AC-5	Network integrity is protected	ZIO-004
PR.DS-2	Data-in-transit is protected	ZIO-001, ZIO-002, ZIO-006
PR.IP-1	A baseline configuration of systems is created and maintained	ZIO-005