Web Application Vulnerability Report

**Scan Date:** 2025-08-01 12:58:27 UTC **Target URL:** https://kb.builtwith.com/general-questions/expired-technology-website/

# Executive Summary

**Scan Results Summary:**- Medium: 4

# Detailed Findings

## 1. Outdated jQuery

**Severity:** Medium **CVSS Score:** CVSS: 5.0 (Medium)

### Description:

Using an outdated jQuery version exposes applications to known security vulnerabilities like XSS attacks, DOM-based vulnerabilities, and cross-site scripting exploits that have been patched in newer versions. These vulnerabilities can allow attackers to inject malicious scripts, steal session cookies, or perform unauthorized actions on behalf of users. The technical impact includes potential data breaches, unauthorized access to user accounts, and complete compromise of client-side application security.

### Proof of Concept:

Version 3.5.1 in use.

### Remediation:

* Upgrade to 3.7.1.

### Business Impact:

\*\*Financial Impact:\*\* A successful exploit could result in significant financial losses through data breach remediation costs, regulatory fines, and potential legal liability from compromised user data, with average breach costs reaching thousands per record in severe cases.  
  
\*\*Reputation Risks:\*\* Public disclosure of a security vulnerability exploiting outdated components can severely damage customer trust and brand reputation, potentially leading to customer attrition and difficulty acquiring new business relationships.  
  
\*\*Compliance Implications:\*\* Depending on the industry, this vulnerability could trigger violations of data protection regulations (GDPR, CCPA, PCI-DSS) and security standards, resulting in substantial regulatory penalties and mandatory disclosure requirements.  
  
\*\*Operational Disruption:\*\* Successful attacks could force emergency system outages, emergency patch deployments, and extensive security audits, disrupting normal business operations and requiring significant IT resources to contain and remediate the incident.

## 2. Outdated Bootstrap

**Severity:** Medium **CVSS Score:** CVSS: 5.0 (Medium)

### Description:

Using an outdated Bootstrap version exposes your application to known vulnerabilities like XSS attacks, CSRF exploits, and insecure default configurations that have been patched in newer releases. The technical impact includes potential data breaches, unauthorized access to user sessions, and compromised client-side security controls that can lead to injection attacks against both users and backend systems. Additionally, outdated versions lack modern security features like improved sanitization, secure default settings, and protection against emerging attack vectors that newer versions address.

### Proof of Concept:

Version 4.3.1 in use.

### Remediation:

* Upgrade to 5.3.3.

### Business Impact:

\*\*Financial Impact\*\*: A security breach exploiting this Bootstrap vulnerability could result in significant costs from data theft, regulatory fines, legal fees, and remediation efforts, potentially reaching hundreds of thousands or millions of dollars depending on the scale of compromise. \*\*Reputation Risk\*\*: Public disclosure of a security vulnerability leading to a breach could severely damage customer trust and brand reputation, particularly if user data is compromised, potentially resulting in customer churn and lost business opportunities. \*\*Compliance Implications\*\*: Organizations handling sensitive data (PII, financial information) may face regulatory violations under frameworks like GDPR, CCPA, or PCI-DSS, leading to substantial penalties and mandatory security audits. \*\*Operational Disruption\*\*: While the CVSS score indicates moderate severity, successful exploitation could lead to service interruptions, forced emergency deployments, and ongoing monitoring requirements that strain IT resources and divert attention from strategic initiatives.

## 3. Outdated Microsoft ASP.NET

**Severity:** Medium **CVSS Score:** CVSS: 5.0 (Medium)

### Description:

Using outdated Microsoft ASP.NET versions exposes applications to known vulnerabilities that Microsoft has already patched in newer releases, including critical security flaws like remote code execution, SQL injection, and cross-site scripting attacks. These older versions lack modern security features such as enhanced encryption protocols, improved authentication mechanisms, and built-in protection against common web application attacks. The technical impact includes potential data breaches, unauthorized system access, and complete application compromise, as attackers can exploit well-documented vulnerabilities for which fixes are readily available but not implemented.

### Proof of Concept:

Version 4.0 in use.

### Remediation:

* Upgrade to 4.8.

### Business Impact:

The outdated Microsoft ASP.NET vulnerability poses significant financial risks through potential data breaches that could result in regulatory fines, legal costs, and remediation expenses, with average data breach costs reaching millions of dollars. Reputation damage could be severe if customer data is compromised, leading to loss of client trust and competitive disadvantage in the marketplace. Compliance implications include violations of data protection regulations like GDPR, HIPAA, or PCI-DSS, potentially resulting in substantial penalties and mandatory security audits. Operationally, the vulnerability creates high disruption risks as successful exploitation could lead to complete application downtime, requiring emergency patching, system rebuilds, and extended recovery periods that impact business continuity.

## 4. CVE-2019-8331 - Bootstrap -

**Severity:** Medium **CVSS Score:** CVSS: 5.0 (Medium)

### Description:

CVE-2019-8331 is a cross-site scripting (XSS) vulnerability in Bootstrap's data-target attribute implementation, specifically affecting versions prior to 3.4.1 and 4.3.1. The vulnerability occurs when the data-target attribute improperly handles user-supplied input, allowing attackers to inject malicious JavaScript code that executes in the context of the victim's browser session. This could enable attackers to steal session cookies, redirect users to malicious sites, or perform unauthorized actions on behalf of authenticated users, making it a critical security risk requiring immediate patching.

### Proof of Concept:

Version: 4.3.1 is affected by CVE-2019-8331

### Remediation:

* Upgrade to the latest patched version.

### Business Impact:

\*\*Financial Impact\*\*: CVE-2019-8331 poses significant financial risks through potential data theft, fraud, and regulatory fines, with remediation costs including emergency patching, code review, and potential legal liabilities from exploited incidents.  
  
\*\*Reputation Risks\*\*: A successful XSS exploit could severely damage customer trust and brand reputation, particularly if user session data is compromised or users are redirected to malicious sites, leading to public exposure and loss of competitive advantage.  
  
\*\*Compliance Implications\*\*: This vulnerability likely violates multiple security standards including PCI DSS, GDPR, and SOC 2 requirements for secure coding practices and XSS protection, potentially resulting in audit failures and regulatory penalties.  
  
\*\*Operational Disruption\*\*: While the CVSS score of 5.0 indicates moderate severity, the XSS nature of this vulnerability can enable privilege escalation and persistent access, potentially leading to ongoing operational disruption until comprehensive patching and security review are completed.