

Claroty JSON SQLi Vulnerabilities

<https://campus.barracuda.com/doc/98216908/>

This article provides an update on the recently discovered JSON-based [SQL Injection Vulnerability](#) by [Team82](#).

The [Claroty T82](#) research team released a [blog](#) last week demonstrating a newly identified SQL injection in JSON-based SQL and how it bypasses many name-brand WAF vendors.

Exploit

The attack technique involves appending JSON syntax to SQL injection payloads. The attack affects only web applications using JSON.

Barracuda Web Application Firewall Mitigation

The Barracuda Web Application Firewall (WAF) protect against this attack with an update in the existing SQL injection category of the Smart Signatures.


The default SQL injection medium and strict checks do not detect this variant, which employs JSON syntax. The new signature detects all identified variants of the JSON syntax-based attacks.


Barracuda Networks has pushed the new signature through Attack Definition Update version 1.222. The [Release Notes](#) have been updated to reflect the changelog.

The Attack Definitions are available only as part of the Energize Updates subscription.

Action Required

1. Set **Automatic Updates** to **ON** for the WAF devices to receive the latest Attack Definition version 1.222.
2. Set the **Operating Mode** for the new attack pattern "*sql-tautology-conditions-json-bypass-string*" to **Active** in the **ADVANCED > View Internal Patterns > Attack Types > sql-injection-medium** group.

BASIC	SECURITY POLICIES	WEBSITES	BOT MITIGATION	ACCESS CONTROL	NETWORKS	ADVANCED	Search help topics 
Backups	Energize Updates	Firmware Update	Export Logs	System Logs	Templates	View Internal Patterns	Libraries
Admin Access Control	High Availability	Appearance	System Configuration	Secure Administration	Troubleshooting	Vulnerability Reports	
CloudGen Firewall Settings	Cloud Control	Task Manager					

Attack Types						Release Notes	Help 
Group	Pattern Name	Pattern Regex	Pattern Algorithm	Case Sensitive	Operating Mode		
cross-site-scripting-strict	opening-html-tag	<([\x08-\x0d\x20\x...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Copy
	arbitrary-tag-injection	(["\'])(\x20 \x09 \x0d ...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	script-string-concat	["\'](\x20 \x09 \x0d ...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	closing-html-tag	<\/([\x08-\x0d\x20\x...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	script-comments	\/*(\s)*\s*\/*		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
sql-injection-medium	sql-tautology-conditions-like-dbcmd	[{ alnum:}]+(OR A...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Copy
	sql-union-command	union.*[{ alnum:}]+...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-tautology-conditions-simple	[{ alnum:}]+(OR A...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-quote-variant	^(\\" ' \`)\$		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-blind-injection	(["\'])(\x09*(or and) \x...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-tautology-conditions-in-dbcmd	[{ alnum:}]+(OR A...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-declare-simple	[{ alnum:}]+(DECL...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-comments	(["\'])(\x08-\x0d\x20 ...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-tautology-conditions-simple-string	[{ alnum:}]+(OR A...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-select-command	((["\'])([" alpha:}]<_]*...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-tautology-conditions-json-bypass-string	("")(x7b)?(")(x7d)... New		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-exec-simple	[{ alnum:}]+(EXEC...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-tautology-conditions-extract	[{ alnum:}]+(OR A...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-command-injection	([" alpha:}]<_*)(i...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	ms-sql-procedures	[{ alnum:}]+<_][sx]p...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-cast-simple	[{ alnum:}]+(VARC...		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details
	sql-quote	(["\'])(\x09*or \x09)		No	<input type="radio"/> Passive <input checked="" type="radio"/> Active <input type="radio"/> Off		Details

This pattern group category is a default setting for all existing profiles (URL and Parameter protections). It is advised to watch out for false positives from this pattern and to contact [Barracuda Networks Technical Support](#) as required.

Related Articles:

- <https://claroty.com/team82/research/js-on-security-off-abusing-json-based-sql-to-bypass-waf>
- <https://securityaffairs.co/wordpress/139445/hacking/web-application-firewalls-waf-bypass.html>
- <https://www.techtarget.com/searchsecurity/news/252528217/Claroty-unveils-web-application-firewall-bypassing-technique>
- <https://www.itworldcanada.com/post/claroty-discovers-method-to-bypass-vendors-web-application-firewalls-waf>
- <https://gbhackers.com/bypass-web-application-firewalls/>

Figures

1. View_Internal_Patterns.png
2. Attack_Types.png
3. Attack_Pattern.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.