About Barracuda Web Application Firewall

With hundreds of lines of code to check - and vulnerabilities often subtle and hard to find - a serious data breach is often the first sign that a web application has problems. Having secured thousands of production applications against more than 11 billion attacks since 2008, the Barracuda Web Application Firewall is the ideal solution for organizations looking to protect web applications from data breaches and defacement. With the Barracuda Web Application Firewall, administrators do not need to wait for clean code or even know how an application works to secure their applications. Organizations can ensure robust security with a Barracuda Web Application Firewall hardware or virtual appliance, deployed either on-premises or in the cloud.

News

Barracuda Campus
campus@barracuda.com

High-Severity OWASSRF exploit in MS Exchange Servers- (CVE-2022-41080 and CVE-2022-41082)

CVE: CVE-2022-41080 | CVSS: 9.8 | Severity: Critical

Description: CVE-2022-41080 vulnerability was discovered in MS Exchange servers 2013, 2016, and 2019. While ProxyNotShell exploit chain used CVE-2022-41040 (SSRF) vulnerability in the Autodiscover endpoint of MS Exchange, and the newfound OWASSRF exploit chain uses CVE-2022-41080 to achieve privilege escalation via MS Exchange Servers.

Barracuda Networks : Barracuda Web Application Firewall and Barracuda Web Application Firewall as a Service (WAFaaS) and Barracuda Load balancer ADC are not vulnerable to the said CVE.

Fix Update:

The fix will be pushed via attackdef for Barracuda Web Application Firewall and Barracuda Load Balancer ADC.

Barracuda WAF-as-a-service accounts will be updated for the definition automatically.

It is advised to watch out for false positives from this pattern and to contact Barracuda Networks Technical Support as required.

Posted on 2023-01-03 22:07:05 modified on 2023-01-09 00:13:21

Barracuda Campus
campus@barracuda.com

Claroty JSON SQLi Vulnerabilities

The Claroty T82 research team released a blog last week demonstrating a newly identified SQL injection in JSON based SQL and how this bypasses many name brand WAF vendors.

While we have had custom patterns available via the Barracuda support teams earlier, we also released an update to our attack signature definitions to explicitly capture these attacks..

ACTION Required : Please make sure that the new attack pattern (In ADVANCED->View Interanl Patterns-> SQL Injection medium group) is in Active operating mode.

For further information, please see the article on Barracuda Campus. Also, for any assistance with the updates or questions regarding the attack patterns, contact Barracuda Networks Technical Support.

Claroty JSON SQLi Vulnerabilities

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 ...

READ ARTICLE

Posted on 2022-12-16 20:28:33 modified on 2022-12-18 23:58:31

Barracuda Campus
campus@barracuda.com

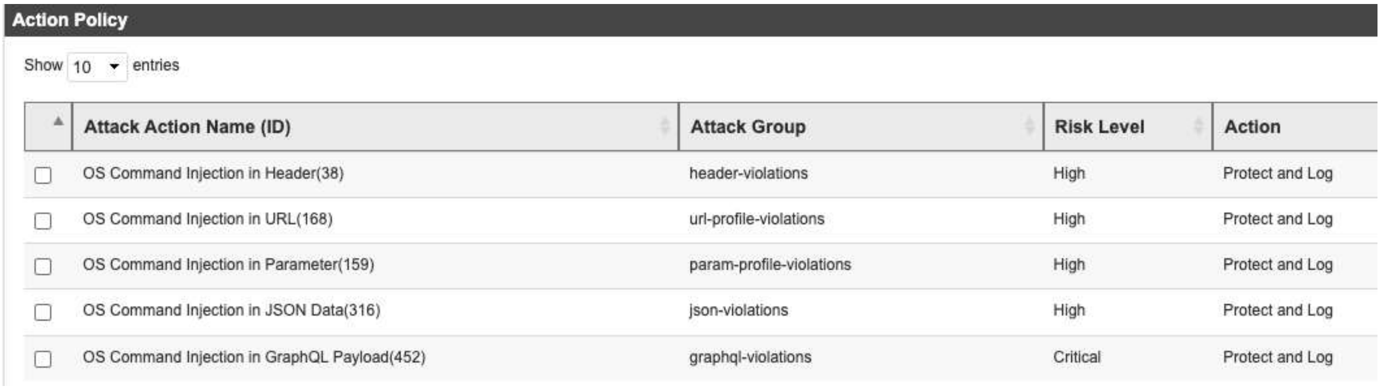
Apache Commons Text packages (CVE-2022-42889)

This article provides an update on the recently discovered vulnerability in Apache Commons Text packages (CVE-2022-42889). This Remote Code Execution (RCE) attack can be carried out on the Apache Commons text packages from version 1.5 until version 1.9.

Barracuda Web Application Firewall, Barracuda WAF-as-a-Service, and Barracuda Load Balancer ADC are not affected by this vulnerability.

Barracuda Web Application Firewall and WAF-as-a-Service protect against this attack out-of-the-box via the existing OS Command injection category of the Smart Signatures.

If you have customised the Action policies, please make sure that the action is not set to *Allow and Log* or *None*.



Action Policy

Show 10 entries

	Attack Action Name (ID)	Attack Group	Risk Level	Action
□	OS Command Injection in Header(38)	header-violations	High	Protect and Log
□	OS Command Injection in URL(168)	url-profile-violations	High	Protect and Log
□	OS Command Injection in Parameter(159)	param-profile-violations	High	Protect and Log
□	OS Command Injection in JSON Data(316)	json-violations	High	Protect and Log
□	OS Command Injection in GraphQL Payload(452)	graphql-violations	Critical	Protect and Log

For any assistance with these settings or questions regarding the attack patterns, contact Barracuda

READ MORE

Posted on 2022-10-20 08:44:51 modified on 2022-11-20 07:46:00

Barracuda Campus
campus@barracuda.com

Barracuda Instructor-led Training Classes available

The Barracuda Campus team is happy to announce that, starting today, we will be offering instructor-led training classes for selected products to all Barracuda partners and customers.

You can now enroll in the courses listed below.
Please click the link to the corresponding course to see the class schedule.

Instructor-led Training Course	Class Duration
CGF01 - Barracuda CloudGen Firewall - Foundation	3 days
CGF0301 - Barracuda CloudGen Firewall – Application Control	1 day
CGF0401 - Barracuda CloudGen Firewall – Advanced WAN Technologies	2 days
CGF0601 - Barracuda CloudGen Firewall – Remote Access	1 day
WAF01 - Barracuda Web Application Firewall - Foundation	2 days
WAF0201 - Barracuda Web Application Firewall – Advanced Features	1 day

Instructor-led Training Course	Class Duration
EP01 - Barracuda Email Protection - Foundation	3 days

READ MORE

Posted on 2022-10-13 02:24:14 modified on 2022-12-15 06:34:23

Barracuda Campus
campus@barracuda.com

Action Required : Microsoft Exchange Zero-Day (CVE-2022-41040 and CVE-2022-41082)

This article provides information on how you can mitigate the newly discovered Zero-day vulnerabilities in Microsoft Exchange Server using Barracuda WAF and Barracuda CloudGen WAF.

These vulnerabilities were published on September 29, 2022, and affect Microsoft Exchange Server 2013, 2016, and 2019. An attacker would need to gain access to the vulnerable system as an authenticated user to exploit these vulnerabilities. CVE-2022-41040 is an SSRF attack that is executed first, to gain access to PowerShell. After that, the attacker can also execute the RCE attack as described in CVE-2022-41082.

Zero-Day Microsoft Exchange Server: Critical Vulnerabilities - OWASSRF and ProxyNotShell

This article provides information on recently discovered zero-day vulnerabilities in the Microsoft Exchange Server versions 2013, 2016, and 2019.The following table provides key information ...

READ ARTICLE

Posted on 2022-09-30 09:50:26 modified on 2022-11-08 23:46:31

Barracuda Campus
campus@barracuda.com

Web Application Firewall Firmware 12 Training Update

The Barracuda Campus team is happy to announce a huge training update:
All online training videos and course materials for Barracuda Web Application Firewall have been updated to firmware 12.
This update also includes all new features introduced with the latest firmware.

BARRACUDA CAMPUS BARRACUDA NETWORKS, INC

Barracuda
Web Application Firewall
Get protection for websites and applications from cyber-threats.

Training

Barracuda Campus provides documentation, training and certification for all Barracuda Networks products.

Read this on campus.barracuda.com >

Posted on 2022-08-04 12:00:40 modified on 2022-08-04 12:01:05

Barracuda Campus
campus@barracuda.com

Barracuda Web Application Firmware 11 - Training Update

The Barracuda Campus team is happy to announce a big training update for Barracuda Web Application Firewall.
All online training videos and course materials have been updated to cover **firmware 11** and all new features introduced with the this firmware release.

Find out more here: https://campus.barracuda.com/product/webapplicationfirewall/learn/

Posted on 2021-09-16 02:15:41

Barracuda Campus
campus@barracuda.com

Web Application Firewall Troubleshooting Training is live

Once again Barracuda Campus has teamed up with our Technical Support to design a training. This time we have identified the most common support requests for Barracuda Web Application Firewall.
In this series of training videos, we’ll show you how to identify these issues and fix them yourself.

Find out more at the link below.

BARRACUDA CAMPUS BARRACUDA NETWORKS, INC

Barracuda
Web Application Firewall
Get protection for websites and applications from cyber-threats.

Training

Barracuda Campus provides documentation, training and certification for all Barracuda Networks products.

Read this on campus.barracuda.com >

Posted on 2021-07-06 23:54:16

LOAD MORE

Documentation

MOST VIEWED RECENTLY UPDATED

Attacks Description - Action Policy

one year ago

Integration with the Barracuda Advanced Threat Protection

one year ago

How to Add an SSL Certificate

7 years ago

Status Codes and Error Responses

7 years ago

Cookie Tampering Attacks Logged When the Barracuda Web Application Firewall Is Initially Deployed

2 years ago

Training

CLASSROOM DISTANCE LEARNING

2023-10-04 09:00 am (GMT+1)

REGISTER

WAF01 Barracuda Web Application Firewall - Foundation

Conducted by **Authorized Training Center**

Hosted at: Fast Lane Institute for Knowledge Transfer GmbH - München, Am Söldnermoos 17, , 85399, Hallbergmoos, DE

Classroom · 2 days · Deutsch

2023-10-06 09:00 am (GMT+1)

REGISTER

WAF0201 Barracuda Web Application Firewall – Advanced Features

Conducted by **Authorized Training Center**

Hosted at: Fast Lane Institute for Knowledge Transfer GmbH - München, Am Söldnermoos 17, , 85399, Hallbergmoos, DE

Classroom · 1 day · Deutsch

BROWSE ALL COURSES

What is Classroom training?

Join instructor-led classroom training conducted by Barracuda Networks, Authorized Training Centers, and Training Partners. Classroom training is offered at various locations around the globe.

BROWSE TRAINING CENTERS

Useful Links

Product Website

Models/Editions

Datasheets

Whitepapers

Community Forum

Product Evaluation

Features

Awards

Case Studies

Frequently Asked Questions

Downloads