// HALBORN

Debridge

Cloudflare Review

Prepared by: **Halborn**

Date of Engagement: **February 7th, 2022 - February 14th, 2022**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	02/14/2022	Alex Yang
0.2	Draft Review	02/15/2022	Gabi Urrutia
1.0	Remediation Plan	05/25/2022	Alex Yang
1.1	Remediation Plan Review	05/26/2022	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Alex Yang	Halborn	Alex.Yang@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

requested Halborn to provide a review of their Cloudflare configuration for best practice.

1.2 AUDIT SUMMARY

In summary, Halborn identified some improvements to reduce the likelihood and impact of multiple risks, which has been mostly addressed by Debridge. The main ones are the following:

- SSL encyrption mode should be full strict
- The proxied websiste should only allow cloudflare's IP address
- SSL Minimum TLS version is 1.2

1.3 TEST APPROACH & METHODOLOGY

Halborn focused on what could be determined using open-source intelligence (OSINT) methods. This involved attempting to identify as many services as possible and determining if they were protected by Cloudflare. The most common mistake we see with DDoS countermeasures is that the services to be protected are also exposed outside Cloudflare and are easily discovered.

RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk

level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

RISK SCALE - LIKELIHOOD

5 - Almost certain an incident will occur.
4 - High probability of an incident occurring.
3 - Potential of a security incident in the long term.
2 - Low probability of an incident occurring.
1 - Very unlikely issue will cause an incident.

RISK SCALE - IMPACT

5 - May cause devastating and unrecoverable impact or loss.
4 - May cause a significant level of impact or loss.
3 - May cause a partial impact or loss to many.
2 - May cause temporary impact or loss.
1 - May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

10 - CRITICAL
9 - 8 - HIGH
7 - 6 - MEDIUM
5 - 4 - LOW
3 - 1 - VERY LOW AND INFORMATIONAL

1.4 SCOPE

This report focuses on the Cloudflare configuration review rather than specifically vulnerabilities as normal.

The following domain is reviewed.
- debridge.finance

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	2	0	2	6

LIKELIHOOD

IMPACT

			(HAL-01) (HAL-02)	
(HAL-03) (HAL-07) (HAL-09) (HAL-10)	(HAL-05)	(HAL-04)		
(HAL-06) (HAL-08)				

EXECUTIVE OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
HAL01 - SSL ENCRYPTION MODE IS FULL	High	SOLVED - 05/20/2022
HAL02 - PROXIED WEBSITE SHOULD ONLY ALLOW CLOUDFLARE'S IP	High	SOLVED - 05/20/2022
HAL03 - SSL/TLS RECOMMENDER IS ON	Low	SOLVED - 05/20/2022
HAL04 - SSL MINIMUM TLS VERSION IS 1.2	Low	SOLVED - 05/20/2022
HAL05 - DNSSEC IS ENABLED	Informational	SOLVED - 05/20/2022
HAL06 - HTST IS ENABLED	Informational	SOLVED - 05/20/2022
HAL07 - CERTIFICATE TRANSPARENCY MONITORING IS ENABLED	Informational	SOLVED - 05/20/2022
HAL08 - HTTP2/3 CAN BE ENABLED	Informational	SOLVED - 05/20/2022
HAL09 - BILLING NOTIFICATION CAN BE ENABLED	Informational	ACKNOWLEDGED
HAL10 - INTERNAL ACCESS WITHOUT VPN VIA CLOUDFLARE	Informational	ACKNOWLEDGED

FINDINGS & TECH DETAILS

3.1 (HAL-01) SSL ENCRYPTION MODE IS FULL - HIGH

Description:

Flexible SSL is enabled under SSL/TLS -> Overview that means Cloudflare can connect to your origin server via HTTP if it doesn't have a valid cert there. Full SSL is recommended here.
Full SSL -> Your origin has a valid certificate (not expired and signed by a trusted CA or Cloudflare Origin CA) installed. Cloudflare will connect over HTTPS and verify the cert on each request.

Recommendation:

Full SSL (strict) should be enabled.

Affected domains:

- debridge.finance

References:
Encryption modes

Remediation Plan:

SOLVED: The deBridge team enabled Full SSL.

3.2 (HAL-02) PROXIED WEBSITE SHOULD ONLY ALLOW CLOUDFLARE'S IP - HIGH

Description:

Your origin server is exposed to the internet directly without Cloudflare, even for non-important websites.

Recommendation:

Recommend to only allow Cloudflare's IP to access your origin server.

Affected domains:

- blog.debridge.finance
- testapi.debridge.finance
- testapiv2.debridge.finance

References:
Cloudflare IP range

Remediation Plan:

SOLVED: The deBridge team now only allows Cloudflare's IP to access to their origin server.

3.3 (HAL-03) SSL/TLS RECOMMENDER IS ON - INFORMATIONAL

Description:

Cloudflare provides an option to check if you can use a more secure SSL/TLS mode.

Recommendation:

Recommend to enable this option to receive update.

Remediation Plan:

SOLVED: The deBridge team enabled SSL/TLS option.

3.4 (HAL-04) SSL MINIMUM TLS VERSION IS 1.2 - LOW

Description:

Minimum TLS Version only allows HTTPS connections from visitors that support the selected TLS protocol version or newer, which may breaks some outdated clients.

Recommendation:

Recommend to enable this option.

Affected domains:

- debridge.finance

References:
minimum tls in cloudflare

Remediation Plan:

SOLVED: The deBridge team enabled a minimum TLS version in CloudFlare.

3.5 (HAL-05) DNSSEC IS ENABLED - LOW

Description:

DNSSEC adds an extra layer of authentication layer to DNS, making sure that visitors go to your domain instead of a spoofed domain.

Recommendation:

Recommend to enable DNSSEC.

Affected domains:

- debridge.finance

References:
Setup DNSSEC

Remediation Plan:

SOLVED: The deBridge team enabled DNSSEC.

3.6 (HAL-06) HSTS IS ENABLED - INFORMATIONAL

Description:

HSTS protects HTTPS web servers from downgrade attacks. These attacks redirect web browsers from an HTTPS web server to an attacker-controlled server, allowing bad actors to compromise user data and cookies.

Recommendation:

Recommend to enable HSTS

Affected domains:

- debridge.finance

References:
Http strict transport security

Remediation Plan:

SOLVED: The deBridge team enabled HTST.

3.7 (HAL-07) CERTIFICATE TRANSPARENCY MONITORING IS ENABLED - INFORMATIONAL

Description:

Receive an email when a Certificate Authority issues a certificate for your domain.

Recommendation:

Recommend to enable this option.

Affected domains:

- debridge.finance

References:
certificate transparency monitoring

Remediation Plan:

SOLVED: The deBridge team enabled certificate transparency monitoring.

3.8 (HAL-08) HTTP2/3 CAN BE ENABLED - INFORMATIONAL

Description:

HTTP/3 is a major revision of the Web's protocol designed to take advantage of QUIC, a new encrypted-by-default Internet transport protocol that provides some improvements designed to accelerate HTTP traffic as well as make it more secure.

Recommendation:

Recommend to enable this option. (Optional)

Affected domains:

- debridge.finance

Remediation Plan:

SOLVED: The deBridge team enabled HTTP2/3.

3.9 (HAL-09) BILLING NOTIFICATION CAN BE ENABLED - INFORMATIONAL

Description:

Adding a billing notification helps team to control your cost in case anything bad happening.

Recommendation:

Recommend to enable this option.

Affected domains:

- debridge.finance

Remediation Plan:

ACKNOWLEDGED: The deBridge team acknowledged this finding.

3.10 (HAL-10) INTERNAL ACCESS WITHOUT VPN VIA CLOUDFLARE - INFORMATIONAL

Description:

Noticed lots of internal application such as sentry, zabbix or dev is exposed to Internet via Cloudflare. We can restrict that access to the internal teams only with Cloudflare Access option.

Recommendation:

Recommend to enable this option which can help team to use SSO for login and auditing.

Affected domains:

- debridge.finance

Remediation Plan:

SOLVED: The deBridge team acknowledged this finding and will fix it in the future.

References:
Cloudflare access without VPN

THANK YOU FOR CHOOSING

// HALBORN