SecurityScorecard

DETAILED REPORT

# Scorecard for Deps

Generated **June 29, 2020**
by Paulo Watanabe (paulo.watanabe@boavistascpc.com.br), Boa Vista Servicos

**About this report**

This report is a point-in-time capture of this Scorecard as of 7:41:35 PM UTC, June 29, 2020. It should not be confused with a pen test result or a final assessment.

**Get the full picture with SecurityScorecard**

SecurityScorecard offers ongoing self-monitoring, history reports, CSV data exports, and more to help security teams protect their organizations. For full free access to your organization's Scorecard, create an account today at bit.ly/2P8okyb.

Learn more about SecurityScorecard at bit.ly/2xXNg4N today.

**What is SecurityScorecard?**

SecurityScorecard is a security ratings service that uses an easy-to-understand A-F grading system to rate companies on their overall security as well as across 10 major risk factors. A company with a C, D, or F rating is 5.4 times more likely to suffer a consequential breach versus A or B-rated companies[1]. Certain risk factors, such as application security and patching cadence, are even more indicative of the likelihood of breach. An F versus an A in these factors may translate into a tenfold increase in the likelihood of a data breach or successful attack.

Learn more about SecurityScorecard's rating system at bit.ly/2zMLSmW.

[1] "New SecurityScorecard Research Can Help You Detect a Data Breach Before It Happens" (https://bit.ly/2yc0JVN)

# Next Steps: Get to an A


**1. Create an account**

This file has a lot of detail but remember, it's only for one point in time. Create an account to get full free access to your organizaton's Scorecard along with continuous self-monitoring, history reports, CSV data exports, and more.

**2. Validate your Digital Footprint**

Once you have an account, review your company's Digital Footprint, the assets SecurityScorecard found as potentially attributable to your company, that affect the ratings in your Scorecard. Request removal or addition of IPs as needed.

**3. Review issue findings**

Investigate the contents of your Scorecard with your team(s). It's a win for your company's security posture when you identify loose ends of which you weren't aware.

**4. Remediate issues, improve your score**

Whether you've deployed a fix, found assets that don't belong to your company, or want to share information about compensating controls, you can let us know by remediating the identified finding(s) and submitting them for resolution approval. Resolutions are handled by our Support team, which will resolve any outstanding item within three business days. Remediate issues within the platform or email support@securityscorecard.com.

# We're here to help

The SecurityScorecard platform is based on transparency and collaboration. Our Customer Reliability Support team provides remediation and resolution services at no charge and are happy to work with you and your customers to resolve any issues. If you need assistance at any stage, get in touch by emailing support@securityscorecard.io.

# Scorecard Overview

B

## Deps

88 Security Score

DOMAIN: deps.com.br

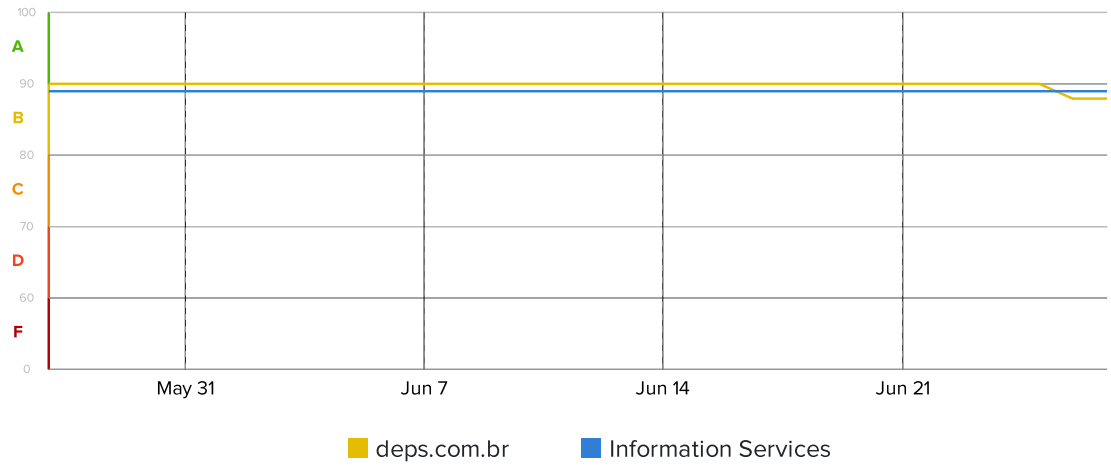
INDUSTRY: INFORMATION SERVICES

### Factors

| | | | | | |
|---|---|---|---|---|---|
| B | 80 | DNS HEALTH | 2 ISSUES | A 100 | CUBIT SCORE | 1 ISSUE |
| A | 100 | IP REPUTATION | 0 ISSUES | A 100 | INFORMATION LEAK | 1 ISSUE |
| B | 85 | NETWORK SECURITY | 2 ISSUES | A 100 | HACKER CHATTER | 0 ISSUES |
| A | 100 | PATCHING CADENCE | 0 ISSUES | A 100 | ENDPOINT SECURITY | 0 ISSUES |
| D | 62 | APPLICATION SECURITY | 8 ISSUES | A 100 | SOCIAL ENGINEERING | 0 ISSUES |

# 30-Day Score History

The chart below shows the evolution of the company's relative security ranking over time. Peaks in score performance represent improvements to overall security, remediation of open isues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.



# Action Items

| FACTOR | SEVERITY | SCORE IMPACT | ISSUES DETECTED |
|---|---|---|---|
| DNS Health | ! | -1.2 | SPF Record Contains a Softfail. Softfail attributes in SPF makes spoofing and phishing email possible. |
| | ! | -1.2 | Malformed SPF Record. The detected SPF record is malformed. |
| Network Security | !! | -1.5 | TLS Protocol Uses Weak Cipher. TLS analysis reveals a weak cipher either through encryption protocol or public key length. |
| | ! | -0.7 | TLS Certificate Without Revocation Control. We observed a TLS certificate that did not contain either CRL or OCSP URLs. |
| Application Security | !!! | -1.9 | Site does not enforce HTTPS. Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code). |
| | !! | -1.5 | Website Does Not Implement HSTS Best Practices. Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website. |
| | !! | -1.2 | Insecure HTTPS Redirect Pattern. Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site. |
| | !! | -1.7 | Website does not implement X-XSS-Protection Best Practices. Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks. |
| | !! | -1.7 | Website does not implement X-Frame-Options Best Practices. Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks. |
| | ! | -0.6 | Website does not implement X-Content-Type-Options Best Practices. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript. |

# B 80 DNS HEALTH

This module measures the health and configuration of a company's DNS settings. It validates that no malicious events occurred in the passive DNS history of the company's network. It also helps validate that mail servers have proper protection in place to avoid spoofing. It also helps verify that DNS servers are configured correctly.

**HIGH SEVERITY**

There are no High Severity Issues for DNS Health

**MEDIUM SEVERITY**

There are no Medium Severity Issues for DNS Health

**LOW SEVERITY**

| | |
|---|---|
| SPF Record Contains a Softfail | 1 |
| Malformed SPF Record | 1 |

**POSITIVE**

There are no Positive Signals for DNS Health

**INFORMATIONAL**

There are no Informational Signals for DNS Health

## SPF Record Contains a Softfail

-1.2 SCORE IMPACT

Softfail attributes in SPF makes spoofing and phishing email possible.

### Description

The Sender Policy Framework (SPF) is an email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record allows a receiving email server to validate that the inbound email comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record in the form of a TXT record. An SPF record with soft fail has been detected; the soft fail attribute enables spoofed email from the domain.

### Recommendation

To resolve this issue, enumerate the list of email servers that are authorized to send email on behalf of the domain. Update the SPF record with the correct email authorization list.

1 finding

| DOMAIN | SPF RECORD | LAST OBSERVED |
|---|---|---|
| deps.com.br | v=spf1 include:spf.protection.outlook.com -all; v=spf1 include:_spf.locaweb.com.br include:_spf.rdstation.com.br ~all | 6/26/2020, 9:23:22 PM |

## Malformed SPF Record

-1.2 SCORE IMPACT

The detected SPF record is malformed.

### Description

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that

### Recommendation

A malformed SPF record can occur as the result of different conditions including: creating multiple SPF records per domain, invalid modifiers, and reaching maximum number of modifiers. The SPF standard can be found at https://tools.ietf.org/html/rfc7208. Additionally, there are tools available at the SPF Project, http://www.openspf.org/Tools.

domain in the form of a specially formatted TXT record. An SPF record is required for spoofed e-mail prevention and anti-spam control.

1 finding

| DOMAIN | SPF RECORD | ANALYSIS | LAST OBSERVED |
|---|---|---|---|
| deps.com.br | v=spf1 include:spf.protection.outlook.com -all; v=spf1 include:_spf.locaweb.com.br include:_spf.rdstation.com.br ~all | Multiple SPF records detected. | 6/26/2020, 9:23:22 PM |

# A 100 IP REPUTATION

The IP Reputation and Malware Exposure module makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds, and third party threat intelligence data sharing partnerships. The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures globally from all over the world. The incoming data is processed and attributed to corporate enterprises. The quantity and duration of malware infections are used as the determining factor for calculating is module the Malware Exposure Key Threat Indicator.

**HIGH SEVERITY**

There are no High Severity Issues for IP Reputation

**MEDIUM SEVERITY**

There are no Medium Severity Issues for IP Reputation

**LOW SEVERITY**

There are no Low Severity Issues for IP Reputation

**POSITIVE**

There are no Positive Signals for IP Reputation

**INFORMATIONAL**

There are no Informational Signals for IP Reputation

No issues found

# B 85 NETWORK SECURITY

The Network Security module checks public datasets for evidence of high risk or insecure open ports within the company network. Insecure ports can often be exploited to allow an attacker to circumvent the login process or obtain elevated access to the system. If misconfigured, the open port can act as the entry point between a hacker's workstation and your internal network

| HIGH SEVERITY | MEDIUM SEVERITY | | LOW SEVERITY | | POSITIVE |
|---|---|---|---|---|---|
| There are no High Severity Issues for Network Security | TLS Protocol Uses Weak Cipher | 1 | TLS Certificate Without Revocation Control | 1 | There are no Positive Signals for Network Security |

**INFORMATIONAL**

There are no Informational Signals for Network Security

## TLS Certificate Without Revocation Control

-0.7 SCORE IMPACT

We observed a TLS certificate that did not contain either CRL or OCSP URLs.

### Description

Certificate revocation lists (CRLs) are files published online by certificate authorities (CAs). These lists indicate which certificates the CA has revoked, invalidating those certificates. TLS clients (e.g., web browsers) may download a CRL, referenced by a TLS server's certificate, to confirm the certificate is currently valid. CAs may operate online certificate status protocol (OCSP) servers, allowing TLS clients to query whether a certificate is currently valid. Responses to OCSP queries may be 'stapled to' (bundled with) certificates by TLS servers. OCSP stapling prevents TLS clients from needing to query the OCSP server themselves, resulting in faster TLS connections. If an attacker acquires the private key corresponding to a certificate, or any other breach of the private key occurs, the CA can use the revocation controls described above to inform TLS clients that the certificate is no longer valid. Certificates that do not contain revocation controls cannot be revoked, and if an attacker acquires the certificate's private key then the certificate will be valid until the expiry date.

### Recommendation

Contact the CA to request that the certificate be reissued with revocation controls.

1 finding

| CERTIFICATE COMMON NAME | CERTIFICATE AUTHORITY | COLLECTION TARGET | PORT | LAST OBSERVED |
|---|---|---|---|---|
| portal.deps.com.br | Let's Encrypt | 201.16.212.4 | 443 | 6/8/2020, 5:47:31 AM |

## TLS Protocol Uses Weak Cipher

-1.5 SCORE IMPACT

TLS analysis reveals a weak cipher either through encryption protocol or public key length.

### Description

The TLS cryptographic configuration being used could be defeated. A symmetric cipher suite is specified by an encryption protocol (e.g. DES, AES). The strength of the encryption used within a Transport Layer Security (TLS) session is determined by the encryption symmetric cipher negotiated between the server and the browser. In order to ensure that only strong cryptographic ciphers are selected the server must be modified to disable the use of weak ciphers and to configure the ciphers in an adequate order. Additionally, as part of the TLS handshake, an asymmetric cipher is utilized. The strength of the asymmetric cipher may be weakened if an insufficient key size is selected.

### Recommendation

It is recommended to configure the server to only support strong symmetric ciphers and to use sufficiently large public key sizes. Specifically, avoid RC4 encryption as there have been multiple vulnerabilities discovered that render it insecure. Additionally, it is recommended to use a public key size of more than 2048 bits.

1 finding

| CERTIFICATE COMMON NAME | COLLECTION TARGET | PORT | LAST OBSERVED |
|---|---|---|---|
| portal.deps.com.br | 201.16.212.4 | 443 | 6/8/2020, 5:47:31 AM |

# A 100 PATCHING CADENCE

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the rate at which it takes a company to remediate and apply patches compared to peers.

**HIGH SEVERITY**

There are no High Severity Issues for Patching Cadence

**MEDIUM SEVERITY**

There are no Medium Severity Issues for Patching Cadence

**LOW SEVERITY**

There are no Low Severity Issues for Patching Cadence

**POSITIVE**

There are no Positive Signals for Patching Cadence

**INFORMATIONAL**

There are no Informational Signals for Patching Cadence

No issues found

# D 62 APPLICATION SECURITY

The Web Application Vulnerability module uses incoming threat intelligence from known exploitable conditions identified via: whitehat CVE databases, blackhat exploit databases, and sensitive findings indexed by major search engines. The module ingests data from multiple public data sets, third party feeds, and an internal proprietary indexing and aggregation engine. The score determines the likelihood of an upcoming web application breach, and checks for any existing defacement code. Presence of vulnerable applications, outdated versions, and active defacements are used to calculate the overall grade.

| HIGH SEVERITY | | MEDIUM SEVERITY | | LOW SEVERITY | | POSITIVE |
|---|---|---|---|---|---|---|
| Site does not enforce HTTPS | 1 | Website Does Not Implement HSTS Best Practices | 3 | Website does not implement X-Content-Type-Options Best Practices | 4 | There are no Positive Signals for Application Security |
| | | Insecure HTTPS Redirect Pattern | 1 | | | |
| | | Website does not implement X-XSS-Protection Best Practices | 4 | | | |
| | | Website does not implement X-Frame-Options Best Practices | 4 | | | |

| INFORMATIONAL | |
|---|---|
| Unsafe Implementation Of Subresource Integrity | 4 |
| Content Security Policy (CSP) Missing | 4 |

## Unsafe Implementation Of Subresource Integrity

Subresource integrity (SRI) is a security feature that enables browsers to verify that files they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing website elements to provide a cryptographic hash that a fetched file must match.

### Description

Many websites that rely on JavaScript and CSS stylesheet files will host these static resources with external organizations (typically CDNs) to improve website load times. Unfortunately, if one of these external organizations is compromised then the JavaScript and CSS files it hosts can also be compromised and used to push malicious code to the original website. Subresource integrity is a way for a website owner to add a checksum value to all externally-hosted files that is used by the browser to verify that files loaded from external organizations have not been modified.

### Recommendation

Please ensure that all website elements (i.e. <script> and <link>) loading JavaScript and CSS stylesheets hosted with external organizations contain the 'integrity' directive with a valid checksum. Example: <script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>

4 findings

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | LAST OBSERVED |
|---|---|---|---|---|
| deps.com.br | https://www.deps.com.br/ | https://deps.com.br/ | https://www.deps.com.br/, 301, https://deps.com.br/ | 6/22/2020, 12:18:30 PM |

Evidence : <script type="text/javascript" src="https://cdnjs.cloudflare.com/ajax/libs/slim-select/1.18.6/slimselect.min.js?ver=5.2.7">,<script type="text/javascript" src="https://cdn.jsdelivr.net/npm/slick-carousel@1.8.1/slick/slick.min.js?ver=5.2.7">,<script src="https://chat.movidesk.com/Scripts/chat-widget.min.js">,<script type="text/javascript" async="" src="https://d335luupugsy2.cloudfront.net/js/loader-scripts/14c2c85c-fa92-465b-b37c-0f3c69861b6c-loader.js">,<link href="https://fonts.googleapis.com/css?family=Encode+Sans+Semi+Condensed&display=swap" rel="stylesheet">,<link rel="stylesheet" id="slim-select-css-css" href="https://cdnjs.cloudflare.com/ajax/libs/slim-select/1.18.6/slimselect.min.css?ver=5.2.7" type="text/css" media="all">,<link rel="stylesheet" id="slick-css-css" href="https://cdn.jsdelivr.net/npm/slick-carousel@1.8.1/slick/slick.css?ver=5.2.7" type="text/css" media="all">,<link href="//fonts.googleapis.com/css?family=PT+Sans:300|PT+Sans:400|PT+Sans:700&display=swap" rel="stylesheet" type="text/css">,<link href="//fonts.googleapis.com/css?family=Open+Sans:300|Open+Sans:400|Open+Sans:700&display=swap" rel="stylesheet" type="text/css">

| | | | | |
|---|---|---|---|---|
| deps.com.br | https://portal.deps.com.br/ | https://portal.deps.com.br/ | n/a | 6/22/2020, 8:10:43 AM |

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | LAST OBSERVED |
|---|---|---|---|---|
| Evidence : <link href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,700" rel="stylesheet">,<link href="https://cdnjs.cloudflare.com/ajax/libs/open-iconic/1.1.1/font/css/open-iconic-bootstrap.min.css" rel="stylesheet" type="text/css"> | | | | |
| deps.com.br | http://webmail.deps.com.br/ | http://webmail.deps.com.br/ | n/a | 6/22/2020, 12:14:05 AM |
| Evidence : <script type="text/javascript" src="//www.googleadservices.com/pagead/conversion.js"> | | | | |
| deps.com.br | https://webmail.deps.com.br/ | https://webmail.deps.com.br/ | n/a | 6/22/2020, 12:14:05 AM |
| Evidence : <script type="text/javascript" src="//www.googleadservices.com/pagead/conversion.js"> | | | | |

## Website does not implement X-Content-Type-Options Best Practices

-0.6 SCORE IMPACT

Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.

### Description

A MIME type is an HTTP header that indicates the type of content returned in a response and how it should be handled and displayed by the browser. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. The X-Content-Type-Options header indicates that browsers should always trust the declared MIME type from the server and not attempt to analyze the content themselves.

### Recommendation

Add the following header to responses from this website: 'X-Content-Type-Options: nosniff'

4 findings

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | https://www.deps.com.br/ | https://deps.com.br/ | https://www.deps.com.br/, 301, https://deps.com.br/ | Header missing | 6/22/2020, 12:18:30 PM |
| Evidence : | | | | | |
| deps.com.br | https://portal.deps.com.br/ | https://portal.deps.com.br/ | n/a | Header missing | 6/22/2020, 8:10:43 AM |
| Evidence : | | | | | |
| deps.com.br | http://webmail.deps.com.br/ | http://webmail.deps.com.br/ | n/a | Header missing | 6/22/2020, 12:14:05 AM |
| Evidence : | | | | | |
| deps.com.br | https://webmail.deps.com.br/ | https://webmail.deps.com.br/ | n/a | Header missing | 6/22/2020, 12:14:05 AM |

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| Evidence : | | | | | |

## Website Does Not Implement HSTS Best Practices

-1.5 SCORE IMPACT

Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.

### Description

HTTP Strict Transport Security is an HTTP header that instructs clients (e.g., web browsers) to only connect to a website over encrypted HTTPS connections. Clients that respect this header will automatically upgrade all connection attempts from HTTP to HTTPS. After a client receives the HSTS header upon its first website visit, future connections to that website are protected against Man-in-the-Middle attacks that attempt to downgrade to an unencrypted HTTP connection. The browser will expire the HTTP Strict Transport Security header after the number of seconds configured in the max-age attribute.

### Recommendation

Every web application (and any URLs traversed to arrive at the website via redirects) should set the HSTS header to remain in effect for at least 12 months (31536000 seconds). It is also recommended to set the 'includeSubDomains' directive so that requests to subdomains are also automatically upgraded to HTTPS. An acceptable HSTS header would declare: Strict-Transport-Security: max-age=31536000; includeSubDomains;

3 findings

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | https://www.deps.com.br/ | https://deps.com.br/ | https://www.deps.com.br/, 301, https://deps.com.br/ | No HSTS header found | 6/22/2020, 12:18:30 PM |
| Evidence : | | | | | |
| deps.com.br | https://portal.deps.com.br/ | https://portal.deps.com.br/ | n/a | No HSTS header found | 6/22/2020, 8:10:43 AM |
| Evidence : | | | | | |
| deps.com.br | https://webmail.deps.com.br/ | https://webmail.deps.com.br/ | n/a | No HSTS header found | 6/22/2020, 12:14:05 AM |
| Evidence : | | | | | |

## Insecure HTTPS Redirect Pattern

-1.2 SCORE IMPACT

Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.

### Description

The HTTP site redirects users to a new URL in a way that cannot be secured with HTTPS and HSTS headers. This leaves users open to man-in-the-middle attackers who can redirect

### Recommendation

Any HTTP site should redirect the user to a secure (i.e. HTTPS) version of the same domain that was originally requested (or a higher-level/parent version of that same domain). For example,

them to a fraudulent/ spoofed version of the intended site. Please see “Site Does Not Enforce HTTPS” issue type for more information regarding man-in-the-middle scenarios.

http://www.example.com should only redirect either to https://www.example.com or https://example.com. This redirect should be done before redirecting to any other domain or subdomain.

1 finding

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | http://www.deps.com.br/ | https://deps.com.br/ | http://www.deps.com.br/ , 302, https://deps.com.br/ | Redirect does not include HSTS header | 6/22/2020, 12:18:30 PM |

Evidence :

## Site does not enforce HTTPS

-1.9 SCORE IMPACT

Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).

### Description

The site responds to HTTP requests without ultimately redirecting the browser to a secure version of the page. Since the site allows plaintext traffic, a man-in-the-middle attacker is able to read and modify any information passed between the site and the user. There are a variety of situations in which an attacker can intercept plaintext traffic in a man-in-the-middle position, including but not limited to: * Open Wi-Fi Hotspots * WPA/WPA2 encrypted hot-spots where the attacker connected before the victim * Malicious Wi-Fi access points * Compromised switches and routers * ARP poisoning on the same wired network It's important to remember that in many of the above situations, an attacker can not only read traffic, but also actively modify the traffic. Even if a site that does not contain sensitive information, an attacker can still inject malicious content to a user’s browser.

### Recommendation

Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.

1 finding

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | LAST OBSERVED |
|---|---|---|---|---|
| deps.com.br | http://webmail.deps.com.br/ | http://webmail.deps.com.br/ | n/a | 6/22/2020, 12:14:05 AM |

## Content Security Policy (CSP) Missing

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user’s browser).

### Description

The Content Security Policy provides a valuable safety net that protects your website from malicious cross-site scripting (XSS) attacks. A well configured policy will stop an attacker attempting to inject their code, or references to other malicious content, into your website. Without a Content Security Policy,

### Recommendation

Enable CSP headers via your webserver configuration.

it's easy for website developers to make mistakes that allow an attacker to inject content that changes the way the website behaves.

4 findings

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | LAST OBSERVED |
|---|---|---|---|---|
| deps.com.br | https://www.deps.com.br/ | https://deps.com.br/ | https://www.deps.com.br/, 301, https://deps.com.br/ | 6/22/2020, 12:18:30 PM |
| Evidence : No content security policy directives found. | | | | |
| deps.com.br | https://portal.deps.com.br/ | https://portal.deps.com.br/ | n/a | 6/22/2020, 8:10:43 AM |
| Evidence : No content security policy directives found. | | | | |
| deps.com.br | http://webmail.deps.com.br/ | http://webmail.deps.com.br/ | n/a | 6/22/2020, 12:14:05 AM |
| Evidence : No content security policy directives found. | | | | |
| deps.com.br | https://webmail.deps.com.br/ | https://webmail.deps.com.br/ | n/a | 6/22/2020, 12:14:05 AM |
| Evidence : No content security policy directives found. | | | | |

## Website does not implement X-XSS-Protection Best Practices

-1.7 SCORE IMPACT

Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.

### Description

The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when websites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP. Without these protections, an attacker can send their victims malicious URLs that inject code into the website

### Recommendation

Add the following header to responses from this website: 'X-XSS-Protection: 1; mode=block'

4 findings

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | https://www.deps.com.br/ | https://deps.com.br/ | https://www.deps.com.br/, 301, https://deps.com.br/ | Header missing | 6/22/2020, 12:18:30 PM |
| Evidence : | | | | | |
| deps.com.br | https://portal.deps.com.br/ | https://portal.deps.com.br/ | n/a | Header missing | 6/22/2020, 8:10:43 AM |

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| Evidence : | | | | | |
| deps.com.br | http://webmail.deps.com.br/ | http://webmail.deps.com.br/ | n/a | Header missing | 6/22/2020, 12:14:05 AM |
| Evidence : | | | | | |
| deps.com.br | https://webmail.deps.com.br/ | https://webmail.deps.com.br/ | n/a | Header missing | 6/22/2020, 12:14:05 AM |
| Evidence : | | | | | |

## Website does not implement X-Frame-Options Best Practices

-1.7 SCORE IMPACT

Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.

### Description

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a '<frame>', '<iframe>' or '<object>'. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other websites.

### Recommendation

Add one of the following headers, using the 'DENY' or 'ALLOW-FROM' directive, to responses from this website: X-Frame-Options: DENY' X-Frame-Options: ALLOW-FROM https://example.com/'

4 findings

| DOMAIN | INITIAL URL | FINAL URL | REQUEST CHAIN | ANALYSIS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | https://www.deps.com.br/ | https://deps.com.br/ | https://www.deps.com.br/, 301, https://deps.com.br/ | Header missing | 6/22/2020, 12:18:30 PM |
| Evidence : | | | | | |
| deps.com.br | https://portal.deps.com.br/ | https://portal.deps.com.br/ | n/a | Header missing | 6/22/2020, 8:10:43 AM |
| Evidence : | | | | | |
| deps.com.br | http://webmail.deps.com.br/ | http://webmail.deps.com.br/ | n/a | Header missing | 6/22/2020, 12:14:05 AM |
| Evidence : | | | | | |
| deps.com.br | https://webmail.deps.com.br/ | https://webmail.deps.com.br/ | n/a | Header missing | 6/22/2020, 12:14:05 AM |
| Evidence : | | | | | |

# A 100 CUBIT SCORE

This proprietary module measures a variety of security issues that a company might have. For example, we check public threat intelligence databases for IP addresses that have been flagged. These misconfigurations may have high exploitability and could cause significant harm to the privacy of your data and infrastructure

**HIGH SEVERITY**

There are no High Severity Issues for Cubit Score

**MEDIUM SEVERITY**

There are no Medium Severity Issues for Cubit Score

**LOW SEVERITY**

There are no Low Severity Issues for Cubit Score

**POSITIVE**

There are no Positive Signals for Cubit Score

**INFORMATIONAL**

| | |
|---|---|
| Possible Typosquat Domains Detected | 12 |

## Possible Typosquat Domains Detected

Domains have been detected which may be an indication of typosquat.

### Description

This is an informational issue and is not calculated as part of the score. Typosquatting, also called URL hijacking, a sting site, or a fake URL, is a form of cybersquatting in which malicious actors register domains that are similar to legitimate domains but contain a common misspelling or a different TLD (Top-Level Domain). This attack relies on the possibility that a user will accidentally mis-type a URL and arrive at the attacker-controlled site instead of their intended destination. In a related practice, called Homograph Attacks, attackers register domains that look visually similar to existing domains (replacing an 'l' with an 'I' or a '1' for example) using similar ASCII characters or in some cases unicode characters that are visually indistinguishable from their equivalent ASCII characters. These attacks can also be used as part of a phishing campaign to deceive email recipients into clicking on a link that leads to an attacker-controlled website. As a best practice, some organizations who utilize brand reputation and domain protection services, may intentionally register similar domains to deter malicious actors from creating typosquatted domains.

### Recommendation

Verify that the typosquat domain does not pose a risk to the organization. If necessary, perform a domain take-down of malicious domains which may be used for phishing.

12 findings

| IP ADDRESS | DOMAIN | LAST OBSERVED |
|---|---|---|
| 198.58.118.167 | smtp.deps.com | 6/26/2020, 2:35:58 AM |
| 96.126.123.244 | mysql.deps.com | 6/26/2020, 2:35:58 AM |
| 45.33.23.183 | ts.deps.com | 6/26/2020, 2:35:58 AM |
| 45.79.19.196 | ftp2.deps.com | 6/26/2020, 2:35:57 AM |

| IP ADDRESS | DOMAIN | LAST OBSERVED |
|---|---|---|
| 104.160.174.169 | ftp.deps.cn | 6/26/2020, 2:35:57 AM |
| 45.79.19.196 | portal.deps.com | 5/28/2020, 3:24:55 PM |
| 198.58.118.167 | mssql.deps.com | 5/28/2020, 3:24:55 PM |
| 172.217.6.115 | mail.dops.com.br | 5/28/2020, 3:24:55 PM |
| 96.126.123.244 | mail.deps.com | 5/28/2020, 3:24:55 PM |
| 45.56.79.23 | imap.deps.com | 5/28/2020, 3:24:55 PM |
| 172.217.17.115 | imap.deeps.com.br | 5/28/2020, 3:24:55 PM |
| 108.179.252.18 | www.depss.com.br | 5/28/2020, 3:24:55 PM |

# A 100 INFORMATION LEAK

This Information Leak module makes use of chatter monitoring and deep web monitoring capabilities to identify compromised credentials being circulated by hackers. These come in the form of bulk data breaches announced publicly as well as smaller breaches, and smaller exchanges between hackers

**HIGH SEVERITY**

There are no High Severity Issues for Information Leak

**MEDIUM SEVERITY**

There are no Medium Severity Issues for Information Leak

**LOW SEVERITY**

There are no Low Severity Issues for Information Leak

**POSITIVE**

There are no Positive Signals for Information Leak

**INFORMATIONAL**

Credentials at Risk 4

## Credentials at Risk

Credentials for accounts associated with employee emails were discovered.

### Description

Accounts with associated emails and passwords, possibly in conjuction with Personally Identifiable Information (PII), have been observed circulating within the hacker underground or the security research community. Reuse of passwords presents an additional security risk. The combination of leaked credentials and credential reuse could lead to the compromise of a corporate system, or any other third-party systems associated with business functions--such as outsourced HR systems, CRMs, or any other SaaS providers used by the business. The credentials below were recovered in the forms of bulk data breach leaks, as well as extracted from public and private Hacker Chatter sources. Leaked PII about employees can also provide information to launch targeted, sophisticated social engineering attacks aimed at affected personnel.

### Recommendation

Ensure employees are not using the affected credentials for any corporate or third-party logins. Ensure that all passwords have been changed since the indication of breach. In the case of corporate passwords, check logs for repeated failed login attempts or repeated password reset attempts from suspicious IP addresses.

4 findings

| DOMAIN | LEAK NAME | LEAK YEAR | DESCRIPTION | AFFECTED USERS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | Linkedin | 2016 | Linkedin is a business social networking service. | simone | 3/15/2020, 12:00:00 PM |
| deps.com.br | Adobe | 2013 | Adobe Systems Incorporated is a computer software company. | pedro | 3/15/2020, 12:00:00 PM |
| deps.com.br | BreachCompilation | 2017 | BreachCompilation is a 1.4 billion compilation of breached credentials. | simone | 3/15/2020, 12:00:00 PM |

| DOMAIN | LEAK NAME | LEAK YEAR | DESCRIPTION | AFFECTED USERS | LAST OBSERVED |
|---|---|---|---|---|---|
| deps.com.br | the-collections | 2019 | Massive dataleaks compilation, from multiple sources, with emails and passwords. | simone | 3/15/2020, 12:00:00 PM |

# A 100 HACKER CHATTER

The SecurityScorecard Hacker Chatter module is an automated collection and aggregation system for the analysis of multiple streams of underground hacker chatter. Forums, IRC, social networks, and other public repositories of hacker community discussions are continuously monitored, collected and aggregated in order to locate mentions of business names and websites. The Hacker Chatter score is an informational indicator ranking that is ranked based on the quantity of indicators that appear within the collection sensors.

**HIGH SEVERITY**

There are no High Severity Issues for Hacker Chatter

**MEDIUM SEVERITY**

There are no Medium Severity Issues for Hacker Chatter

**LOW SEVERITY**

There are no Low Severity Issues for Hacker Chatter

**POSITIVE**

There are no Positive Signals for Hacker Chatter

**INFORMATIONAL**

There are no Informational Signals for Hacker Chatter

No issues found

# A 100 ENDPOINT SECURITY

The Endpoint Security Module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins. The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

**HIGH SEVERITY**

There are no High Severity Issues for Endpoint Security

**MEDIUM SEVERITY**

There are no Medium Severity Issues for Endpoint Security

**LOW SEVERITY**

There are no Low Severity Issues for Endpoint Security

**POSITIVE**

There are no Positive Signals for Endpoint Security

**INFORMATIONAL**

There are no Informational Signals for Endpoint Security

No issues found

# A 100 SOCIAL ENGINEERING

The SecurityScorecard Social Engineering Module is used to determine the potential susceptibility of an organization to a targeted social engineering attack. The Social Engineering module ingests data from social networks and public data breaches, and blends proprietary analysis methods. The Social Engineering Score is an informational indicator calculated based on the quantity of indicators that appear in SecurityScorecard collection sensors.

**HIGH SEVERITY**

There are no High Severity Issues for Social Engineering

**MEDIUM SEVERITY**

There are no Medium Severity Issues for Social Engineering

**LOW SEVERITY**

There are no Low Severity Issues for Social Engineering

**POSITIVE**

There are no Positive Signals for Social Engineering

**INFORMATIONAL**

There are no Informational Signals for Social Engineering

No issues found

No content (including ratings, data, reports, software or other application or output therefrom) or any part thereof (collectively, Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system without the prior written permission of SecurityScorecard, Inc. (SSC) The Content shall not be used for any unlawful or unauthorized purposes.

SSC and any third-parties, and their directors, officers, shareholders, employees, customers and agents (collectively SSC Parties) do not guarantee or warrant the accuracy, completeness, timeliness or availability of the Content. SSC Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of the Content. The Content is provided on an "as is" basis. SSC PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS,(3) FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall SSC Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

USERS OF THE CONTENT MUST USE ALL REASONABLE ENDEAVORS TO MITIGATE ANY LOSS OR DAMAGE WHATSOEVER (AND HOWSOEVER ARISING) AND NOTHING HEREIN SHALL BE DEEMED TO RELIEVE OR ABROGATE USERS OF ANY SUCH DUTY TO MITIGATE ANY LOSS OR DAMAGE.

IN ANY EVENT, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF THE SSC PARTIES FOR ANY REASON WHATSOEVER RELATED TO ACCESS TO OR USE OF CONTENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL AMOUNT PAID TO SSC BY THE USER FOR SERVICES PROVIDED DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY, AND (B) U.S. $100.

Security-related analyses, including ratings and statements in the Content, are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SSC’s opinions, analyses and ratings should not be relied on as a substitute for the skill, judgment and experience of the user and its management, employees, advisors and clients when making business decisions. SSC assumes no obligation to update the Content following publication in any form or format. While SSC has obtained information from sources it believes to be reliable, SSC does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Users expressly agree that (a) the security ratings and other security opinions provided via the Content do not reflect, identify or detect every vulnerability or security issue or address any other risk; (b) the security ratings and other opinions provided do not take into account users’ particular objectives, situations or needs; (c) each rating or other opinion will be weighed, if at all, solely as one factor in any decision made by or on behalf of any user; and (d) users will accordingly, with due care, make their own study and evaluation of the risks of doing business with any entity. If a user identifies any in the Content, we invite you to share that information with us by emailing us at support@securityscorecard.io. 