SecurityScorecard

DETAILED REPORT

Scorecard for Ravenswood Family Health Center

Generated **March 4, 2021**
by Tiffany Yan (tyan@gaig.com), Great American Insurance Group

About this report

This report is a point-in-time capture of this Scorecard as of 8:50:43 PM UTC, March 4, 2021. 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.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

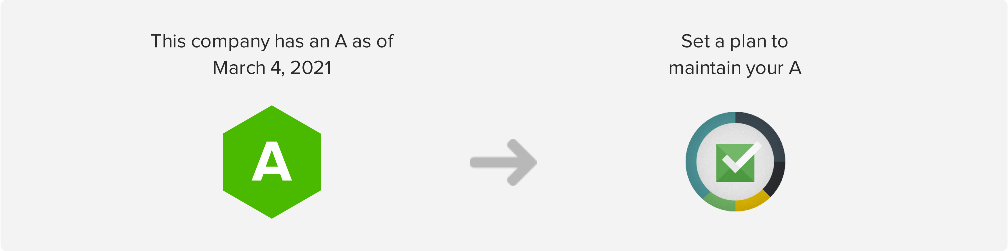
What is SecurityScorecard?

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: Stay at an A


This company has an A as of March 4, 2021

Set a plan to maintain your 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. Spot new issues, maintain your A

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.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company’s Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

Scorecard Overview

A

Ravenswood Family Health Center

90 Security Score

DOMAIN: ravenswoodfhc.org

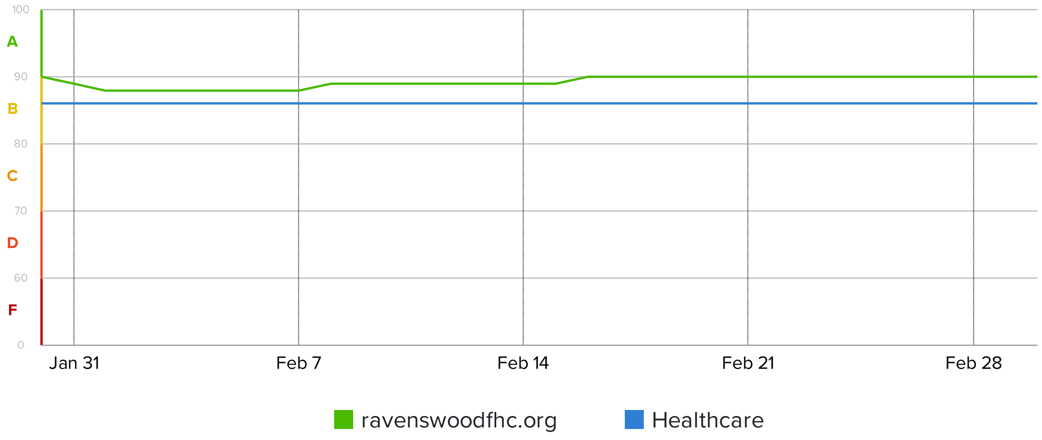
INDUSTRY: HEALTHCARE

Factors

C	71	APPLICATION SECURITY	7 ISSUES
A	100	CUBIT SCORE	0 ISSUES
A	90	DNS HEALTH	1 ISSUE
A	100	ENDPOINT SECURITY	0 ISSUES
A	100	HACKER CHATTER	0 ISSUES
A	100	IP REPUTATION	0 ISSUES
A	100	INFORMATION LEAK	0 ISSUES
B	85	NETWORK SECURITY	2 ISSUES
A	100	PATCHING CADENCE	0 ISSUES
A	100	SOCIAL ENGINEERING	1 ISSUE

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.



Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

Action Items

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
Application Security	!!!	-3.3	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).
	!!	-1.6	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.
	!!	-1.8	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.
	!	-0.3	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.
	!	-0.5	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.
DNS Health	!	-0.8	SPF Record Contains Wildcard. Wildcard attributes in SPF make spoof email possible.
Network Security	!!	-1.0	RDP Service Observed. We observed RDP, a remote access service, publicly exposed.
	!!	-0.9	TLS Service Supports Weak Cipher Suite. A TLS service was observed supporting weak cipher suites.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

C 71 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	
Content Security Policy (CSP) Missing	6

!! MEDIUM SEVERITY	
Insecure HTTPS Redirect Pattern	2
Website Does Not Implement HSTS Best Practices	6

! LOW SEVERITY	
Website does not implement X-XSS-Protection Best Practices	2
Website does not implement X-Frame-Options Best Practices	4
Website does not implement X-Content-Type-Options Best Practices	6

✓ POSITIVE

There are no Positive Signals for Application Security

i INFORMATIONAL	
Unsafe Implementation Of Subresource Integrity	4

!!! Content Security Policy (CSP) Missing

-3.3 SCORE IMPACT

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

Recommendation

Enable CSP headers via your webserver configuration.

6 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
ravenswoodfhc.org	https://mail.ravenswoodfhc.org/	https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://mail.ravenswoodfhc.org/, 302, https://mail.ravenswoodfhc.org/owa/, 302, https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	3/1/2021, 2:58:31 PM
Evidence : No content security policy directives found.				
ravenswoodfhc.org	http://www.ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://www.ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	3/1/2021, 9:35:08 AM
Evidence : No content security policy directives found.				
ravenswoodfhc.org	https://www.ravenswoodfhc.org/	https://ravenswoodfhc.org/	https://www.ravenswoodfhc.org/, 301, https://ravenswoodfhc.org/	3/1/2021, 9:35:08 AM
Evidence : No content security policy directives found.				

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
ravenswoodfhc.org	https://webmail.ravenswoodfhc.org/	https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://webmail.ravenswoodfhc.org/, 302, https://webmail.ravenswoodfhc.org/owa/, 302, https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	3/1/2021, 7:48:38 AM
Evidence : No content security policy directives found.				
ravenswoodfhc.org	https://ravenswoodfhc.org/	https://ravenswoodfhc.org/	n/a	2/28/2021, 12:22:02 PM
Evidence : No content security policy directives found.				
ravenswoodfhc.org	http://ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	2/28/2021, 12:22:02 PM
Evidence : No content security policy directives found.				

Website does not implement X-XSS-Protection Best Practices

-0.3 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'

2 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
ravenswoodfhc.org	https://mail.ravenswoodfhc.org/	https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://mail.ravenswoodfhc.org/, 302, https://mail.ravenswoodfhc.org/owa/, 302, https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	Header missing	3/1/2021, 2:58:31 PM
Evidence :					
ravenswoodfhc.org	https://webmail.ravenswoodfhc.org/	https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://webmail.ravenswoodfhc.org/, 302, https://webmail.ravenswoodfhc.org/owa/, 302, https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	Header missing	3/1/2021, 7:48:38 AM
Evidence :					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

‼ Insecure HTTPS Redirect Pattern

-1.6 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 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.

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, 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.

2 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
ravenswoodfhc.org	http://www.ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://www.ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Redirect goes to different apex domain	3/1/2021, 9:35:08 AM
Evidence :					
ravenswoodfhc.org	http://ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Redirect goes to different apex domain	2/28/2021, 12:22:02 PM
Evidence :					

‼ Website Does Not Implement HSTS Best Practices

-1.8 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;

6 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
ravenswoodfhc.org	https://mail.ravenswoodfhc.org/	https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://mail.ravenswoodfhc.org/, 302, https://mail.ravenswoodfhc.org/owa/, 302, https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	No HSTS header found	3/1/2021, 2:58:31 PM
Evidence :					
ravenswoodfhc.org	http://www.ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://www.ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Header missing includeSubDomains directive	3/1/2021, 9:35:08 AM
Evidence : Strict-Transport-Security: max-age=31536000					
ravenswoodfhc.org	https://www.ravenswoodfhc.org/	https://ravenswoodfhc.org/	https://www.ravenswoodfhc.org/, 301, https://ravenswoodfhc.org/	Header missing includeSubDomains directive	3/1/2021, 9:35:08 AM
Evidence : Strict-Transport-Security: max-age=31536000					
ravenswoodfhc.org	https://webmail.ravenswoodfhc.org/	https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://webmail.ravenswoodfhc.org/, 302, https://webmail.ravenswoodfhc.org/owa/, 302, https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	No HSTS header found	3/1/2021, 7:48:38 AM
Evidence :					
ravenswoodfhc.org	https://ravenswoodfhc.org/	https://ravenswoodfhc.org/	n/a	Header missing includeSubDomains directive	2/28/2021, 12:22:02 PM
Evidence : Strict-Transport-Security: max-age=31536000					
ravenswoodfhc.org	http://ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Header missing includeSubDomains directive	2/28/2021, 12:22:02 PM
Evidence : Strict-Transport-Security: max-age=31536000					

Website does not implement X-Frame-Options Best Practices

-0.5 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
ravenswoodfhc.org	http://www.ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://www.ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Header missing	3/1/2021, 9:35:08 AM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
ravenswoodfhc.org	https://www.ravenswoodfhc.org/	https://ravenswoodfhc.org/	https://www.ravenswoodfhc.org/, 301, https://ravenswoodfhc.org/	Header missing	3/1/2021, 9:35:08 AM
Evidence :					
ravenswoodfhc.org	https://ravenswoodfhc.org/	https://ravenswoodfhc.org/	n/a	Header missing	2/28/2021, 12:22:02 PM
Evidence :					
ravenswoodfhc.org	http://ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Header missing	2/28/2021, 12:22:02 PM
Evidence :					

! 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'

6 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
ravenswoodfhc.org	https://mail.ravenswoodfhc.org/	https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://mail.ravenswoodfhc.org/, 302, https://mail.ravenswoodfhc.org/owa/, 302, https://mail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fmail.ravenswoodfhc.org%2fowa%2f&reason=0	Header missing	3/1/2021, 2:58:31 PM
Evidence :					
ravenswoodfhc.org	http://www.ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://www.ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Header missing	3/1/2021, 9:35:08 AM
Evidence :					
ravenswoodfhc.org	https://www.ravenswoodfhc.org/	https://ravenswoodfhc.org/	https://www.ravenswoodfhc.org/, 301, https://ravenswoodfhc.org/	Header missing	3/1/2021, 9:35:08 AM
Evidence :					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
ravenswoodfhc.org	https://webmail.ravenswoodfhc.org/	https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	https://webmail.ravenswoodfhc.org/, 302, https://webmail.ravenswoodfhc.org/owa/, 302, https://webmail.ravenswoodfhc.org/owa/auth/logon.aspx?url=https%3a%2f%2fwebmail.ravenswoodfhc.org%2fowa%2f&reason=0	Header missing	3/1/2021, 7:48:38 AM
Evidence :					
ravenswoodfhc.org	https://ravenswoodfhc.org/	https://ravenswoodfhc.org/	n/a	Header missing	2/28/2021, 12:22:02 PM
Evidence :					
ravenswoodfhc.org	http://ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	Header missing	2/28/2021, 12:22:02 PM
Evidence :					

ⓘ 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
ravenswoodfhc.org	http://www.ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://www.ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	3/1/2021, 9:35:08 AM
Evidence : <link href="//fonts.googleapis.com/css?family=Heebo:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Manrope:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i&amp;subset=latin&amp;display=swap" rel="stylesheet" media="none" onload="media=&quot;all&quot;">				
ravenswoodfhc.org	https://www.ravenswoodfhc.org/	https://ravenswoodfhc.org/	https://www.ravenswoodfhc.org/, 301, https://ravenswoodfhc.org/	3/1/2021, 9:35:08 AM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
Evidence : <link href="//fonts.googleapis.com/css?family=Heebo:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Manrope:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i&amp;subset=latin&amp;display=swap" rel="stylesheet" media="none" onload="media=&quot;all&quot;">				
ravenswoodfhc.org	https://ravenswoodfhc.org/	https://ravenswoodfhc.org/	n/a	2/28/2021, 12:22:02 PM
Evidence : <link href="//fonts.googleapis.com/css?family=Heebo:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Manrope:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i&amp;subset=latin&amp;display=swap" rel="stylesheet" media="none" onload="media=&quot;all&quot;">				
ravenswoodfhc.org	http://ravenswoodfhc.org/	https://ravenswoodfhn.org/	http://ravenswoodfhc.org/, 301, https://ravenswoodfhn.org/	2/28/2021, 12:22:02 PM
Evidence : <link href="//fonts.googleapis.com/css?family=Heebo:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Manrope:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic&amp;display=swap" rel="stylesheet">,<link href="//fonts.googleapis.com/css?family=Poppins:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i&amp;subset=latin&amp;display=swap" rel="stylesheet" media="none" onload="media=&quot;all&quot;">				

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

i INFORMATIONAL

There are no Informational Signals for Cubit Score

No issues found

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

A 90 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 Wildcard 1

✓ POSITIVE

There are no Positive Signals for DNS Health

i INFORMATIONAL

There are no Informational Signals for DNS Health

! SPF Record Contains Wildcard

-0.8 SCORE IMPACT

Wildcard attributes in SPF make spoof email possible.

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 domain in the form of a specially formatted TXT record. An SPF record is required for spoofed email prevention and anti-spam control. However, if a wildcard pass attribute is included, it is still possible to spoof email from a particular domain. An SPF record has been detected for 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
ravenswoodfhc.org		3/2/2021, 5:10:41 PM

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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

i INFORMATIONAL

There are no Informational Signals for Endpoint Security

No issues found

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

i INFORMATIONAL

There are no Informational Signals for Hacker Chatter

No issues found

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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

i INFORMATIONAL

There are no Informational Signals for IP Reputation

No issues found

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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

i INFORMATIONAL

There are no Informational Signals for Information Leak

No issues found

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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

There are no High Severity Issues for Network Security

!! MEDIUM SEVERITY

RDP Service Observed	1
TLS Service Supports Weak Cipher Suite	2

! LOW SEVERITY

There are no Low Severity Issues for Network Security

✓ POSITIVE

There are no Positive Signals for Network Security

i INFORMATIONAL

There are no Informational Signals for Network Security

!! RDP Service Observed

-1.0 SCORE IMPACT

We observed RDP, a remote access service, publicly exposed.

Description

The RDP protocol offers remote access to a host, providing a view of the host's console as output and accepting keyboard and mouse events as input.
We observed an RDP service on the Internet, accessible by the public. Remote access services are attractive targets to attackers because they provide remote control over a host. Once logged-in, users can install programs, access files, and run commands on the host. Attackers can add hosts over which they have gained control to botnets, adding the host's computational capabilities and bandwidth to their spam, malware, or distributed denial-of-service (DDoS) campaigns. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Due to sharing user authentication databases with other Microsoft services, brute-forcing this service may provide credentials useful on other services. Attackers may launch denial-of-service (DoS) attacks against the service, rendering the service unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

Recommendation

Exposing remote access services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

1 finding

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Microsoft Terminal Services	50.206.186.67	3389	1/24/2021, 2:07:12 PM

!! TLS Service Supports Weak Cipher Suite

-0.9 SCORE IMPACT

A TLS service was observed supporting weak cipher suites.

Description

Transport Layer Security (TLS), the successor to Secure Socket Layer (SSL), is a network protocol that encrypt communications between TLS servers (e.g., websites) and TLS clients (e.g., web browsers). Every communication is secured by a cipher suite: a combination of several algorithms working in concert. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. Consensus on which algorithms are untrustworthy evolves over time, and if a communication is protected with a weak cipher suite then that communication can be altered or decrypted.

Recommendation

Disable the cipher suites listed in the evidence column of the measurement.

2 findings

TARGET	PORT	OBSERVATIONS	LAST OBSERVED
vpn.ravenswoodfhc.org	443	3	2/15/2021, 8:11:22 PM
12.219.157.139	443	3	2/9/2021, 5:19:10 AM

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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

i INFORMATIONAL

There are no Informational Signals for Patching Cadence

No issues found

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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

i INFORMATIONAL

Exposed Personal Information (Historical)	12

i Exposed Personal Information (Historical)

Personal information for individuals associated with employee emails were exposed.

Description

Social engineering attacks are significantly more effective when they are used in combination with exposed personal information. For example, security questions to reset account passwords, or to recover accounts that require personal information. Additionally, it's easier for hackers to impersonate employees to gain higher level access. Please note that SecurityScorecard only sees the categories of information associated with exposure.
For privacy reasons, affected user names are only visible to the Administrator of the respective account and are not displayed for other scorecards than you follow.

Recommendation

It's not feasible to remove the information off the internet once exposed so mitigation against social engineering attacks are recommended. Ensure that:
* employees have regular cyber security awareness training * protocols are established for handling sensitive information * periodic, unannounced, tests are performed.

12 findings

DOMAIN	LEAK NAME	LEAK YEAR	DESCRIPTION	AFFECTED USERS	LAST OBSERVED
ravenswoodfhc.org	MGM Resorts	2019	The breach included 10.6M guest records with 3.1M unique email addresses stemming back to 2017. The exposed data included email and physical addresses, names, phone numbers and dates of birth		2/24/2020, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

DOMAIN	LEAK NAME	LEAK YEAR	DESCRIPTION	AFFECTED USERS	LAST OBSERVED
ravenswoodfhc.org	RankWatch.com	2016	RankWatch is an SEO marketing platform that gives a way for companies to see all the aspects of digital and Internet marketing used. The leak is from a exposed mongoDB and looks like most of the information was gathered, probably by scrappers and other 3party apps. More then 40Million emails and other information got leaked.		8/31/2019, 12:00:00 AM
ravenswoodfhc.org	ApexSMS	2018	ApexSMS is a SMS text marketing company that also tracks user. This company suffered a data breach that leaked more then 8M clients information		6/10/2019, 12:00:00 AM
ravenswoodfhc.org	verifications.io	2019	verifications.io provides a service of Email Validation and Verification, Data Enhancement, and Free Phone Lookup. more info: https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service/		3/13/2019, 12:00:00 AM
ravenswoodfhc.org	data-contacts	2018	Unknown source. Exposed elasticsearch instance, possibly related to medical industry.		2/1/2019, 12:00:00 AM
ravenswoodfhc.org	datanleads.com	2018	DATA & LEADS, INC is a website that sell data on company and people - https://blog.hackenproof.com/industry-news/new-data-breach-exposes-57-million-records		12/10/2018, 12:00:00 AM
ravenswoodfhc.org	pdlCollection	2018	Unknown origin, pdlCollection have scrapped data from Linkedin and possible other sources.		12/4/2018, 12:00:00 AM
ravenswoodfhc.org	pdlCollection	2018	Unknown origin, pdlCollection have scrapped data from Linkedin and possible other sources.		12/4/2018, 12:00:00 AM
ravenswoodfhc.org	pdlCollection	2018	Unknown origin, pdlCollection have scrapped data from Linkedin and possible other sources.		12/3/2018, 12:00:00 AM
ravenswoodfhc.org	pdlCollection	2018	Unknown origin, pdlCollection have scrapped data from Linkedin and possible other sources.		12/3/2018, 12:00:00 AM

DOMAIN	LEAK NAME	LEAK YEAR	DESCRIPTION	AFFECTED USERS	LAST OBSERVED
ravenswoodfhc.org	Adapt.io	2018	Adapt.io is a website that provide a business contact database. https://blog.hacken.io/how-sensitive-is-your-non-sensitive-data		11/19/2018, 12:00:00 AM
ravenswoodfhc.org	Customers Live	2018	Unknown source, but seems like a marketing related database, containing information of referals and points		11/8/2018, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent 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 toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.

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. ©2021 SecurityScorecard, Inc. All rights reserved.