# SecurityScorecard

## ISSUES REPORT FOR

# New York University

**This report was prepared on 3/15/2020 by SecurityScorecard.**

SecurityScorecard's cutting-edge platform collects threat and vulnerability data, analyzes and processes it across 10 major, security categories using proprietary, non-invasive risk collection techniques.

If you have any questions about your report or want to get an updated report, please feel free to contact us at support@securityscorecard.io.

Learn more at securityscorecard.com

## SCORECARD OVERVIEW

C

# New York University

74% Security Score

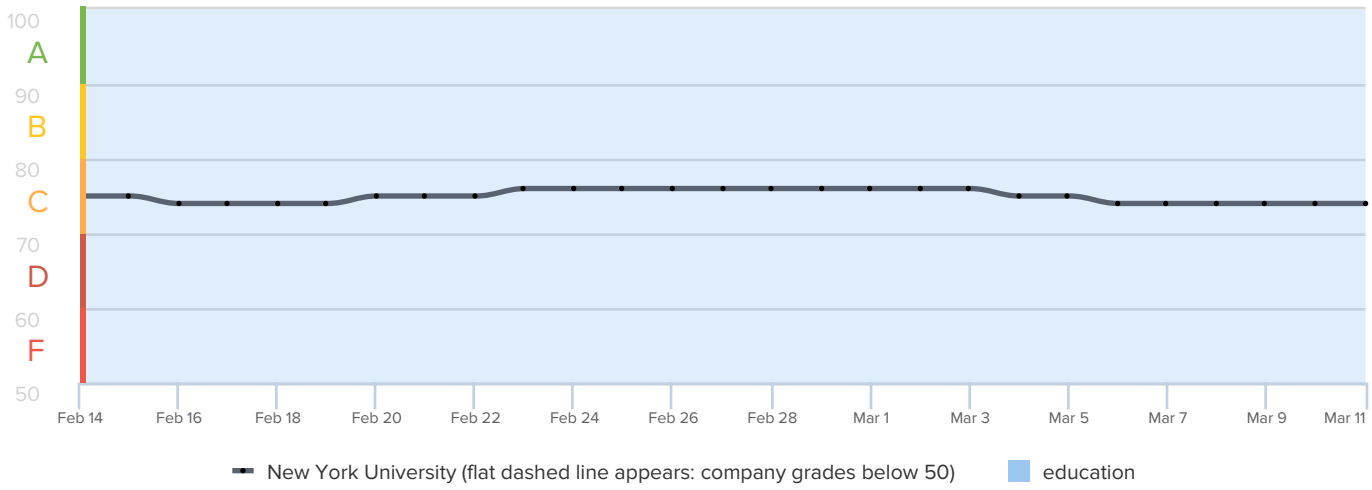
DOMAIN: nyu.edu

INDUSTRY: Education

| | | | | | |
|---|---|---|---|---|---|
| D | 65 | NETWORK SECURITY | 21 ISSUES | | |
| D | 69 | DNS HEALTH | 2 ISSUES | | |
| C | 70 | PATCHING CADENCE | 8 ISSUES | | |
| C | 72 | ENDPOINT SECURITY | 2 ISSUES | | |
| C | 77 | IP REPUTATION | 3 ISSUES | | |
| C | 72 | APPLICATION SECURITY | 14 ISSUES | | |
| A | 100 | CUBIT SCORE | 1 ISSUE | | |
| A | 100 | HACKER CHATTER | 0 ISSUES | | |
| A | 100 | INFORMATION LEAK | 0 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. The shaded area represents the range of values taken by companies in the education industry.




Peaks in score performance represent improvements to overall security posture, remediation of open issues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.

# ACTION ITEMS

| FACTOR | SEVERITY | ISSUES DETECTED |
|---|---|---|
| Cubit Score | i | Possible Typosquat Domains Detected. Domains have been detected which may be an indication of typosquat. |
| IP Reputation | !!! | Malware Events, Last Day. Communications indicative of malware infections were observed over the last 24 hours. |
| | !! | Malware Events, Last Month. Communications indicative of malware infections were observed over the last 30 days. |
| | ! | Malware Events, Last Year. Communications indicative of malware infections were observed over the last 365 days. |
| Endpoint Security | !! | Outdated Web Browser Observed. An outdated web browser connected to a web server. |
| | !! | Outdated Operating System Observed. A web browser on an outdated operating system connected to a web server. |
| Application Security | !!! | 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). |
| | !! | 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. |
| | !! | Redirect Chain Contains HTTP. Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site. |
| | !! | 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. |
| | !! | 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. |
| | !! | 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. |
| | ! | 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. |
| | i | Content Security Policy Contains Broad Directives. 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). |

| | | |
|---|---|---|
| | ⓘ | Website References Object Storage. Objects (files) stored in object storage buckets (storage partitions) can be downloaded, referenced, and used by websites. |
| | ⓘ | Website Hosted on Object Storage. Many object storage services offer hosting for a website's static assets. Amazon S3's documentation can be found at https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html. |
| | ⓘ | 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). |
| | ⓘ | Content Security Policy Contains 'unsafe-*' Directive. 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). |
| | ⓘ | 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. |
| | ✓ | Web Application Firewall (WAF) Detected. A web application firewall (WAF) monitors traffic to and from a web application, and attempts to detect and block traffic associated with common malicious behaviors. A WAF is an important defensive layer that helps secure your web application. |
| Patching Cadence | !!! | High-Severity Vulnerability in Last Observation. We observed a high-severity vulnerability during our last scan, which may still be publicly exposed. |

| FACTOR | SEVERITY | ISSUES DETECTED |
|---|---|---|
| Patching Cadence | !!! | High Severity CVEs Patching Cadence. High severity vulnerability seen on network more than 30 days after CVE was published. |
| | !! | Medium Severity CVEs Patching Cadence. Medium severity vulnerability seen on network more than 60 days after CVE was published. |
| | !! | End-of-Service Product. We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed. |
| | !! | End-of-Life Product. We observed an end-of-life product, one that is no longer developed or sold, publicly exposed. |
| | !! | Medium-Severity Vulnerability in Last Observation. We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed. |
| | ! | Low Severity CVEs Patching Cadence. Low severity vulnerability seen network more than 180 days after CVE was published. |
| | ! | Low-Severity Vulnerability in Last Observation. We observed a low-severity vulnerability during our last scan, which may still be publicly exposed. |
| DNS Health | !! | SPF Record Missing. A missing SPF record has been detected for a domain. |
| | ! | SPF Record Contains a Softfail. Softfail attributes in SPF makes spoofing and phishing email possible. |
| Network Security | !!! | Certificate Is Revoked. Revoked certificates prevent TLS clients from connecting to servers. |
| | !!! | SSH Software Supports Vulnerable Protocol. Server(s) observed running SSH software that support an SSH protocol lower than version 2. |
| | !!! | MongoDB Service Observed. We observed MongoDB, a database management system, publicly exposed. |
| | !! | MySQL Service Observed. We observed MySQL, a database management system, publicly exposed. |
| | !! | rsync Service Observed. We observed rsync, a file-sharing service, publicly exposed. |
| | !! | Certificate Is Self-Signed. Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients. |
| | !! | SMB Service Observed. We observed SMB, a file and printer-sharing service, publicly exposed. |
| | !! | RDP Service Observed. We observed RDP, a remote access service, publicly exposed. |
| | !! | Certificate Is Expired. Expired certificates prevent TLS clients from connecting to servers. |
| | !! | VNC Service Observed. We observed VNC, a remote access service, publicly exposed. |
| | !! | IMAP Service Observed. We observed IMAP, an email retrieval service, publicly exposed. |

| FACTOR | SEVERITY | ISSUES DETECTED |
|---|---|---|
| Network Security | !! | SSH Supports Weak MAC. A weak Message Authentication Code (MAC) algorithm has been detected. |
| | !! | SSH Supports Weak Cipher. A weak cipher has been detected. |
| | !! | TLS Protocol Uses Weak Cipher. TLS analysis reveals a weak cipher either through encryption protocol or public key length. |
| | ! | FTP Service Observed. We observed FTP, a file-sharing service, publicly exposed. |
| | ! | Certificate Lifetime Is Longer Than Best Practices. We observed a certificate with a lifetime longer than 39 Months. |
| | ! | Telnet Service Observed. We observed Telnet, a remote access service, publicly exposed. |
| | ! | TLS Certificate Without Revocation Control. We observed a TLS certificate that did not contain either CRL or OCSP URLs. |
| | i | POP3 Service Observed. We observed POP3, an email retrieval service, publicly exposed. |
| | ✓ | Extended Validation Certificate Observed. The organization has undergone an extended identity-validation process when acquiring a certificate. |

| | | |
|---|---|---|
| | ✓ | TLS Certificate Status Request ("OCSP Stapling") Detected. The organization has taken additional steps to include revocation information with their TLS Certificate response. |

# D 65 NETWORK SECURITY

## ABOUT THIS FACTOR

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

| | |
|---|---|
| SSH Software Supports Vulnerable Protocol | 11 |
| Certificate Is Revoked | 2 |
| MongoDB Service Observed | 2 |
| Elasticsearch Service Observed | 0 |

### MEDIUM SEVERITY

| | |
|---|---|
| TLS Protocol Uses Weak Cipher | 82 |
| Certificate Is Expired | 53 |
| Certificate Is Self-Signed | 4 |
| SSH Supports Weak Cipher | 502 |
| SSH Supports Weak MAC | 109 |
| VNC Service Observed | 190 |
| SMB Service Observed | 2 |
| rsync Service Observed | 5 |
| RDP Service Observed | 10 |
| MySQL Service Observed | 33 |
| IMAP Service Observed | 27 |
| Apache Cassandra Service Observed | 0 |
| Apache CouchDB Service Observed | 0 |
| Microsoft SQL Server Service Observed | 0 |
| PostgreSQL Service Observed | 0 |
| Redis Service Observed | 0 |
| SSL Certificate Uses Weak Signature | 0 |

### LOW SEVERITY

| | |
|---|---|
| Certificate Lifetime Is Longer Than Best Practices | 12 |
| Telnet Service Observed | 16 |
| FTP Service Observed | 58 |
| TLS Certificate Without Revocation Control | 55 |

### POSITIVE SIGNALS

| | |
|---|---|
| TLS Certificate Status Request ("OCSP Stapling") Detected | 51 |
| Extended Validation Certificate Observed | 2 |
| DDoS Protection Service Detected | 0 |

### INFORMATIONAL

| | |
|---|---|
| POP3 Service Observed | 28 |
| Open TCP Ports Observed | 0 |

NETWORK SECURITY > ISSUE DETAIL

# SSH Supports Weak Cipher

**A weak cipher has been detected.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

## RECOMMENDATION

Configure the SSH server to disable Arcfour and CBC ciphers.

## ABOUT THIS ISSUE

The SSH server is configured to support either Arcfour or Cipher Block Chaining (CBC) mode cipher algorithms. SSH can be configured to use Counter (CTR) mode encryption instead of CBC. The use of Arcfour algorithms should be disabled.

NETWORK SECURITY > ISSUE DETAIL

## SSH Supports Weak MAC

**A weak Message Authentication Code (MAC) algorithm has been detected.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Configure the SSH server to disable the use of MD5.

### ABOUT THIS ISSUE

The SSH server is configured to support MD5 algorithm. The cryptographic strength depends upon the size of the key and algorithm that is used. A Modern MAC algorithms such as SHA1 or SHA2 should be used instead.

NETWORK SECURITY > ISSUE DETAIL

## IMAP Service Observed

**We observed IMAP, an email retrieval service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Review the business necessity of hosting a public IMAP server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

### ABOUT THIS ISSUE

The IMAP protocol offers access to messages stored on email servers. IMAP servers frequently contain all messages ever sent or received by an email account, not just recent messages. We observed an IMAP service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. 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 access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

## MySQL Service Observed

**We observed MySQL, a database management system, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Exposing database 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.

### ABOUT THIS ISSUE

MySQL is an open-source database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a MySQL service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. 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. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

## RDP Service Observed

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

To request more details regarding this issue, please contact *success@securityscorecard.io*

### 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.

### ABOUT THIS ISSUE

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.

NETWORK SECURITY > ISSUE DETAIL

## rsync Service Observed

**We observed rsync, a file-sharing service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Exposing rsync 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.

### ABOUT THIS ISSUE

The rsync protocol provides an efficient method of transferring files between hosts. The rsync service offers access to files stored on servers, giving users the ability to upload, download, and delete files. The rsync daemon does not support encryption, exposing all uploaded and downloaded files to man-in-the-middle attacks. We observed an rsync daemon on the Internet, accessible by the public. File-sharing services are attractive targets to attackers due to the data they may contain. An attacker that gains access to the files on an rsync server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached rsync server may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. 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. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

## SMB Service Observed

**We observed SMB, a file and printer-sharing service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Exposing SMB 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.

### ABOUT THIS ISSUE

The SMB protocol offers access to files, printers, and other services on a network. We observed an SMB service on the Internet, accessible by the public. These services are attractive targets to attackers due to the data they may contain, and the potential for access to other network resources. 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.

NETWORK SECURITY > ISSUE DETAIL

# VNC Service Observed

**We observed VNC, a remote access service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### 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.

### ABOUT THIS ISSUE

The VNC 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 a VNC 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. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

# Certificate Is Expired

**Expired certificates prevent TLS clients from connecting to servers.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Services presenting expired certificates should cause noticeable failures, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored. Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

### ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Certificates are digital assets that require renewal or decommissioning on a schedule.

NETWORK SECURITY > ISSUE DETAIL

## Certificate Is Self-Signed

**Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Services presenting self-signed certificates should cause noticeable failures or user-visible warnings, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact your CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored.

### ABOUT THIS ISSUE

When a certificate is issued, it is 'signed' by a certificate authority (CA). Signatures are attestations of the certificate-holder's identity. TLS clients (e.g., web browsers) maintain trust stores, which are lists of CAs whose attestations they trust. The ability to sign a certificate may be delegated from a CA to another entity, such as a subsidiary, creating chains of attestations. In the context of chains of attestation, the delegating CA is the root CA, and the delegated CA is the intermediate CA. Trust stores in TLS clients may contain both intermediate and root CAs. TLS clients validate a server's certificate by tracing its chain of attestations back to a CA in its trust store. Certificates that are self-signed have no chain of attestations: they are self-attested. This means that most TLS clients, when presented with a self-signed certificate, will display a warning before connecting to the server, or refuse to connect to the server. Off-the-shelf software and hardware frequently runs services that use self-signed certificates by default. Many of these services can be configured to use certificates that are not self-signed. The use of self-signed certificates may result in TLS clients being configured to skip validating certificates, making their connections vulnerable to man-in-the-middle attacks. Users that bypass their web browser's warning upon connecting to a server presenting a self-signed certificate are also vulnerable to man-in-the-middle attacks. Self-signed certificates have narrow, but legitimate use cases, such as protecting services whose clients are configured to use public key pinning.

NETWORK SECURITY > ISSUE DETAIL

## TLS Protocol Uses Weak Cipher

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

To request more details regarding this issue, please contact *success@securityscorecard.io*

### 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.

### ABOUT THIS ISSUE

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.

NETWORK SECURITY > ISSUE DETAIL

## FTP Service Observed

**We observed FTP, a file-sharing service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Review the business necessity of hosting a public FTP server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

### ABOUT THIS ISSUE

The FTP protocol offers access to files stored on servers, giving users the ability to upload, download, and delete files. Many FTP servers are used by automated processes, and are neglected or poorly-configured. Modern protocols, such as SFTP, provide better security than FTP. We observed an FTP service on the Internet, accessible by the public. File-sharing services are attractive targets to attackers due to the data they may contain. An attacker that gains access to the files on an FTP server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached FTP server may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. 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. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

## Telnet Service Observed

**We observed Telnet, a remote access service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Telnet is an inherently unsafe protocol. Remove the service from the Internet. If a remote access service is necessary, replace Telnet with SSH if possible. If not possible, often the case with older networked hardware, ensure the service is only accessible by VPN.

### ABOUT THIS ISSUE

Insecure and/or suspicious Telnet open ports have been detected as being publicly accessible. The availability of these ports allow attackers to engage in authentication bypass attacks (such as brute forcing attempts, remote buffer overflows, blank passwords). An attacker can leverage this access to pivot access into further enterprise resources.

NETWORK SECURITY > ISSUE DETAIL

## Certificate Lifetime Is Longer Than Best Practices

**We observed a certificate with a lifetime longer than 39 Months.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Contact the CA and arrange the issuance of a new certificate with a lifetime that does not exceed 39 months.

**ABOUT THIS ISSUE**

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. New algorithms and versions of algorithms with larger key sizes are created regularly, and the best practices surrounding certificates evolve with them. The Certificate Authority and Browser forum, an industry group that sets standards surrounding the creation and use of certificates, has decided to limit the lifetime of certificates to 39 months. This means that CAs who are members of the forum are required to issue certificates with lifetimes that do not exceed 39 months.

NETWORK SECURITY > ISSUE DETAIL

## TLS Certificate Without Revocation Control

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

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

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

**ABOUT THIS ISSUE**

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.

NETWORK SECURITY > ISSUE DETAIL

## Extended Validation Certificate Observed

**The organization has undergone an extended identity-validation process when acquiring a certificate.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

EV certificates should be strongly considered by organizations if their users are likely to be targeted by phishing attacks. Phishing attacks often use typosquatted domain names (e.g., exanple.com versus example.com). Users of legitimate sites, who are accustomed to the visual indicators associated with EV certificates are more likely to notice such attacks.

### ABOUT THIS ISSUE

Certificate Authorities (CAs) issue certificates according to a variety of policies, and embed within each certificate a reference to the policy under which it was issued. The type of policy that offers the most assurance of the certificate-holder's identity is called an extended validation (EV) policy, and certificates issued under these policies are called EV certificates. To receive an EV certificate, an organization must prove to a CA that it is a currently-operating legal entity, along with several other attributes. EV certificates provide the highest level of assurance currently available. TLS clients (e.g., web browsers) consider EV certificates to be more trustworthy than certificates issued under other policies. Most web browsers display visual indicators a user is viewing a website secured with an EV certificate. Visual indicators provide additional assurance to the user that website they are viewing belongs to the company they intended to visit.

NETWORK SECURITY > ISSUE DETAIL

## POP3 Service Observed

**We observed POP3, an email retrieval service, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Review the business necessity of hosting a public POP3 server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

**ABOUT THIS ISSUE**

The POP3 protocol offers access to messages stored on email servers. POP3 servers typically contain only the most recent messages received by an email account, deleting the messages from the server once they are downloaded by a user. The use of POP3 may complicate BCP/DR due to each individual user being responsible for the entirety of their email history. We observed a POP3 service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. 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 access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

# D 69 DNS HEALTH

## ABOUT THIS FACTOR

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 | | MEDIUM SEVERITY | | LOW SEVERITY | |
|---|---|---|---|---|---|
| Open DNS Resolver Detected | 0 | SPF Record Missing | 74 | SPF Record Contains a Softfail | 2 |
| | | | | Malformed SPF Record | 0 |
| | | | | SPF Record Contains Wildcard | 0 |

**POSITIVE SIGNALS**

| | |
|---|---|
| Valid DNSSEC Configuration Detected | 0 |

**INFORMATIONAL**

*There are no Info Risk Issues to detect for DNS Health*

DNS HEALTH > ISSUE DETAIL

## SPF Record Missing

**A missing SPF record has been detected for a domain.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Create a valid Sender Policy Framework (SPF) record. Ensure the configuration of the SPF DNS record to verify syntax and MTA servers. Test the configuration to make sure its valid by checking the header of an incoming email looking for "spf=pass" Allow for DNS caching during testing; it may take up to 48 hours to fully propagate across the Internet. The nature of the SMTP protocol does not allow for complete prevention of spoofed emails, however the SPF header will reveal whether the email is authentic.

### ABOUT THIS ISSUE

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 e-mail prevention and anti-spam control.

DNS HEALTH > ISSUE DETAIL

## SPF Record Contains a Softfail

**Softfail attributes in SPF makes spoofing and phishing email possible.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**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.

**ABOUT THIS ISSUE**

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.

# C 70 PATCHING CADENCE

## ABOUT THIS FACTOR

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 | | MEDIUM SEVERITY | | LOW SEVERITY | |
|---|---|---|---|---|---|
| High-Severity Vulnerability in Last Observation | 160 | Medium-Severity Vulnerability in Last Observation | 1525 | Low-Severity Vulnerability in Last Observation | 24 |
| High Severity CVEs Patching Cadence | 169 | End-of-Service Product | 1 | Low Severity CVEs Patching Cadence | 6 |
| | | End-of-Life Product | 1 | | |
| | | Medium Severity CVEs Patching Cadence | 881 | | |

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for Patching Cadence*

**INFORMATIONAL**

*There are no Info Risk Issues to detect for Patching Cadence*

PATCHING CADENCE > ISSUE DETAIL

## High-Severity Vulnerability in Last Observation

**We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

### ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

## High Severity CVEs Patching Cadence

**High severity vulnerability seen on network more than 30 days after CVE was published.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

**ABOUT THIS ISSUE**

Based on scan data, the company had high severity CVE vulnerability that was open longer than 30 days after the CVE was published. High severity CVEs are those with a documented CVSS severity over 7.0. It is best practice in standards such as PCI DSS to mitigate or patch high severity vulnerabilities within 30 days. Details on each vulnerability are listed in the table below.

PATCHING CADENCE > ISSUE DETAIL

## Medium-Severity Vulnerability in Last Observation

**We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

**ABOUT THIS ISSUE**

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

## End-of-Life Product

**We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Ensure the affected product has an extended support contract that includes security patches. Review the vendor's statement of EOL guidelines for replacement products and upgrade to a new product line or manufacturer.

**ABOUT THIS ISSUE**

A product that has been declared as end-of-life (EOL) by the manufacturer has been detected. An EOL product is no longer marketed, sold, or upgraded by the manufacturer. Products at this stage in their life cycle are more likely to have vulnerabilities that will remain unpatched.

PATCHING CADENCE > ISSUE DETAIL

## End-of-Service Product

**We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Replace or upgrade the affected product. Review the vendor's statement of EOS guidelines for replacement products or contact the vendor. In some cases, it may be possible to negotiate a custom support plan for the EOS product.

### ABOUT THIS ISSUE

A product that has been declared as end-of-service (EOS) by the manufacturer has been detected. An EOS product is no longer eligible for any support, security patches, or replacement parts. Products at this stage in their life cycle are more likely to have vulnerabilities that need to be patched, but without service support those vulnerabilities will persist until the product is replaced. Using EOS products also violates several compliance frameworks, including PCI DSS and HIPAA.

PATCHING CADENCE > ISSUE DETAIL

## Medium Severity CVEs Patching Cadence

**Medium severity vulnerability seen on network more than 60 days after CVE was published.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

### ABOUT THIS ISSUE

Based on scan data, the company had medium severity CVE vulnerability that was open longer than 60 days after the CVE was published. Medium severity CVEs are those with a documented CVSS severity between 4.0 and 6.9. It is best practice to mitigate or patch medium severity vulnerabilities within 60 days. Details on each vulnerability are listed in the table below.

PATCHING CADENCE > ISSUE DETAIL

## Low-Severity Vulnerability in Last Observation

**We observed a low-severity vulnerability during our last scan, which may still be publicly exposed.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

**ABOUT THIS ISSUE**

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

## Low Severity CVEs Patching Cadence

**Low severity vulnerability seen network more than 180 days after CVE was published.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

**ABOUT THIS ISSUE**

Based on scan data, the company had low severity CVE vulnerability that was open longer than 180 days after the CVE was published. Low severity CVEs are those with a documented CVSS severity under 4.0. It is best practice to mitigate or patch high severity vulnerabilities within 180 days. Details on each vulnerability are listed in the table below.

# C 72 ENDPOINT SECURITY

## ABOUT THIS FACTOR

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 Risk Issues to detect for Endpoint Security*

**MEDIUM SEVERITY**

| | |
|---|---|
| Outdated Web Browser Observed | 1074 |
| Outdated Operating System Observed | 1 |

**LOW SEVERITY**

*There are no Low Risk Issues to detect for Endpoint Security*

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for Endpoint Security*

**INFORMATIONAL**

| | |
|---|---|
| Multiple Browsers Detected | 0 |

ENDPOINT SECURITY > ISSUE DETAIL

# Outdated Web Browser Observed

**An outdated web browser connected to a web server.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

## RECOMMENDATION

Update the web browsers in question. Enable automatic updates if available from your web browser vendor and permitted in your environment.

## ABOUT THIS ISSUE

The web is constantly evolving, using different languages, protocols, and file formats over time. Web browsers regularly release new versions, on time scales as short as every six weeks. These new versions frequently contain security and stability fixes. When a web browser connects to a web server, it informs the server its platform and version information. This information assists the server in providing appropriate content. The information can also be recorded and aggregated to determine what platforms and browser versions are being used by hosts at various places on the Internet. Using such a data set, it was found that an outdated web browser was in use as described in the table below. Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or NAT gateway with a single external IP will appear to be the source of an entire network full of corporate desktops.

ENDPOINT SECURITY > ISSUE DETAIL

# Outdated Operating System Observed

**A web browser on an outdated operating system connected to a web server.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Update affected device's operating system. Enable automatic updates if available from your software vendor and permitted in your environment. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

### ABOUT THIS ISSUE

When a web browser connects to a web server, it informs the server its platform and version information. This information assists the server in providing appropriate content. The information can also be recorded and aggregated to determine what platforms and browser versions are being used by hosts at various places on the Internet. Using such a data set, it was found that an outdated operating system was in use as described in the table below. Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or NAT gateway with a single external IP will appear to be the source of an entire network full of corporate desktops.

# C 77 IP REPUTATION

## ABOUT THIS FACTOR

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 | | MEDIUM SEVERITY | | LOW SEVERITY | |
|---|---|---|---|---|---|
| Malware Events, Last Day | 2 | Malware Events, Last Month | 13 | Malware Events, Last Year | 53 |
| | | P2P Activities | 0 | | |
| | | Attack Detected | 0 | | |

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for IP Reputation*

**INFORMATIONAL**

| | |
|---|---|
| Tor Exit Nodes | 0 |
| Unsolicited Commercial Email | 0 |

IP REPUTATION > ISSUE DETAIL

## Malware Events, Last Day

**Communications indicative of malware infections were observed over the last 24 hours.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### RECOMMENDATION

Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

### ABOUT THIS ISSUE

After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.

IP REPUTATION > ISSUE DETAIL

## Malware Events, Last Month

**Communications indicative of malware infections were observed over the last 30 days.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

**ABOUT THIS ISSUE**

After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.

IP REPUTATION > ISSUE DETAIL

## Malware Events, Last Year

**Communications indicative of malware infections were observed over the last 365 days.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

**ABOUT THIS ISSUE**

After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.

# C 72 APPLICATION SECURITY

## ABOUT THIS FACTOR

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

| | |
|---|---|
| Site does not enforce HTTPS | 7 |
| High Severity Content Management System vulnerabilities identified | 0 |

### MEDIUM SEVERITY

| | |
|---|---|
| Website does not implement X-XSS-Protection Best Practices | 26 |
| Website does not implement X-Frame-Options Best Practices | 21 |
| Redirect Chain Contains HTTP | 4 |
| Insecure HTTPS Redirect Pattern | 5 |
| Website Does Not Implement HSTS Best Practices | 34 |
| Medium Severity Content Management System vulnerabilities identified | 0 |

### LOW SEVERITY

| | |
|---|---|
| Website does not implement X-Content-Type-Options Best Practices | 26 |
| Session Cookie Missing 'HttpOnly' Attribute | 0 |
| Cookie Missing 'Secure' Attribute | 0 |
| Low Severity Content Management System vulnerabilities identified | 0 |

### POSITIVE SIGNALS

| | |
|---|---|
| Web Application Firewall (WAF) Detected | 16 |
| Domain Uses HSTS Preloading | 0 |

### INFORMATIONAL

| | |
|---|---|
| Website References Object Storage | 6 |
| Website Hosted on Object Storage | 1 |
| Unsafe Implementation Of Subresource Integrity | 17 |
| Content Security Policy Contains Broad Directives | 2 |
| Content Security Policy Contains 'unsafe-*' Directive | 2 |
| Content Security Policy (CSP) Missing | 26 |
| Object Storage Bucket with Risky ACL | 0 |

APPLICATION SECURITY > ISSUE DETAIL

## 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.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

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

**ABOUT THIS ISSUE**

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

APPLICATION SECURITY > ISSUE DETAIL

## 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.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

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

**ABOUT THIS ISSUE**

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.

APPLICATION SECURITY > ISSUE DETAIL

## Web Application Firewall (WAF) Detected

**A web application firewall (WAF) monitors traffic to and from a web application, and attempts to detect and block traffic associated with common malicious behaviors. A WAF is an important defensive layer that helps secure your web application.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Companies should consider implementing a web application firewall that can protect against common web vulnerabilities, such as SQL Injection and cross-site scripting (XSS). Many hosting providers offer WAF capabilities as well.

**ABOUT THIS ISSUE**

A well configured WAF can detect and block a wide variety of attacks. Capabilities vary between products, but at minimum most WAFs can block SQL injection and Cross Site Scripting attacks. A WAF is no substitute to a well-designed web application that is not vulnerable to these attacks in the first place, but it still plays an important role in providing layered security.

APPLICATION SECURITY > ISSUE DETAIL

## 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).**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Enable CSP headers via your webserver configuration.

**ABOUT THIS ISSUE**

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.

APPLICATION SECURITY > ISSUE DETAIL

## Content Security Policy Contains Broad Directives

**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).**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Explicitly specify trusted sources for your script-src and object-src policies. Ideally you can use the 'self' directive to limit scripts and objects to only those on your own domain, or you can explicitly specify domains that you trust and rely upon for your site to function.

**ABOUT THIS ISSUE**

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from loading resources on your page from domains that you don't explicitly trust. However, by using overly broad methods of describing what you trust (ie. 'http:', '*', 'http://*') for your script-src and object-src directives, or your default-src directive in the absence of those directives, this key feature of the CSP header can be bypassed by an attacker.

APPLICATION SECURITY > ISSUE DETAIL

## Content Security Policy Contains 'unsafe-*' Directive

**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).**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Remove the unsafe directives from the content security policy. For trusted resources that must be used inline with HTML, you can use nonces or hashes in your content security policy's source list to mark the resources as trusted. Nonces are randomly generated numbers placed with inline content that you trust. By including the nonce in both the content and the header, the browser knows to trust the script. Example inline script with a nonce: <script nonce=aBFef03nceIOfn39hr3rsatsdfa>alert('Hello, world.');</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'nonce-aBFef03nceIOfn39hr3rsatsdfa' Warning: For nonces to be effective, they must be randomly regenerated every time the page is loaded. If an attacker can guess the nonce value, the protection is useless. Hashes work similarly to nonces, but only need to be generated once. By taking the hash of a script and including it in the header, it will mark the script as trusted. If the attacker tries to change the script, the hash will change and it will no longer be trusted. Example inline script to be hashed: <script>alert('Hello, world.');</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'sha256-qznLcsROx4GACP2dm0UCKCzCG-HiZ1guq6ZZDob_Tng='

**ABOUT THIS ISSUE**

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from running code embedded within the HTML of your site. However, the use of unsafe-eval and unsafe-inline policies in the CSP prevent this key safety feature from functioning. These unsafe directives mean that, should the site be vulnerable to XSS or HTML injection attacks, the attacker will be able to inject their own resources directly into the HTML response and have the browser execute them.

APPLICATION SECURITY > ISSUE DETAIL

## 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.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

### 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;

### ABOUT THIS ISSUE

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.

APPLICATION SECURITY > ISSUE DETAIL

## 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).**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

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

**ABOUT THIS ISSUE**

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.

APPLICATION SECURITY > ISSUE DETAIL

## 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.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**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.

**ABOUT THIS ISSUE**

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.

APPLICATION SECURITY > ISSUE DETAIL

## Redirect Chain Contains HTTP

**Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Any HTTP site should immediately redirect users to HTTPS-protected URLs and ensure that any further redirects do not occur over HTTP. Prefer the usage of HTTPS URLs over HTTP when available, avoiding an unnecessary redirect.

**ABOUT THIS ISSUE**

While redirecting a user to their ultimate URL destination, the user passes through one or more URLs served over HTTP (instead of HTTPS). Having HTTP links in a redirect chain weakens other security technologies (e.g., HTTPS and HSTS headers) that are deployed elsewhere in the chain.

APPLICATION SECURITY > ISSUE DETAIL

## 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.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**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>

**ABOUT THIS ISSUE**

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 inject 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.

APPLICATION SECURITY > ISSUE DETAIL

## 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.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**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/'

**ABOUT THIS ISSUE**

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.

APPLICATION SECURITY > ISSUE DETAIL

## Website Hosted on Object Storage

**Many object storage services offer hosting for a website's static assets. Amazon S3's documentation can be found at https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Ensure that the usage of external services, such as Amazon S3, conforms to company policies.

**ABOUT THIS ISSUE**

There is no risk in using object storage services in this fashion. However, if the Access Control List (ACL) on the bucket (storage partition) the website is hosted on is misconfigured, then the website may be compromised or defaced by attackers.

APPLICATION SECURITY > ISSUE DETAIL

## Website References Object Storage

**Objects (files) stored in object storage buckets (storage partitions) can be downloaded, referenced, and used by websites.**

To request more details regarding this issue, please contact *success@securityscorecard.io*

**RECOMMENDATION**

Ensure that the usage of external services, such as Amazon S3, conforms to company policies.

**ABOUT THIS ISSUE**

There is no risk in using object storage services in this fashion. However, if the Access Control List (ACL) on the bucket (storage partition) the website is hosted on is misconfigured, then the website may be compromised or defaced by attackers.

# A 100 CUBIT SCORE

## ABOUT THIS FACTOR

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 Risk Issues to detect for Cubit Score*

**MEDIUM SEVERITY**

*There are no Medium Risk Issues to detect for Cubit Score*

**LOW SEVERITY**

| | |
|---|---|
| Exposed Subdomain | 0 |

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for Cubit Score*

**INFORMATIONAL**

| | |
|---|---|
| Possible Typosquat Domains Detected | 25 |

CUBIT SCORE > ISSUE DETAIL

# Possible Typosquat Domains Detected

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

To request more details regarding this issue, please contact *success@securityscorecard.io*

## 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.

## ABOUT THIS ISSUE

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.

# A 100 HACKER CHATTER

## ABOUT THIS FACTOR

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 Risk Issues to detect for Hacker Chatter*

**MEDIUM SEVERITY**

| | |
|---|---|
| Booter Shells Identified | 0 |
| Defacement | 0 |

**LOW SEVERITY**

*There are no Low Risk Issues to detect for Hacker Chatter*

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for Hacker Chatter*

**INFORMATIONAL**

| | |
|---|---|
| Hacker Chatter Mention | 0 |

No issues found.

## A 100 INFORMATION LEAK

### ABOUT THIS FACTOR

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 Risk Issues to detect for Information Leak*

**MEDIUM SEVERITY**

*There are no Medium Risk Issues to detect for Information Leak*

**LOW SEVERITY**

| | |
|---|---|
| Sensitive Application Information Exposed (GitHub) | 0 |
| Sensitive Application Information Exposed (Google) | 0 |
| Credentials at Risk | 0 |

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for Information Leak*

**INFORMATIONAL**

*There are no Info Risk Issues to detect for Information Leak*

No issues found.

## A 100 SOCIAL ENGINEERING

### ABOUT THIS FACTOR

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 Risk Issues to detect for Social Engineering*

**MEDIUM SEVERITY**

*There are no Medium Risk Issues to detect for Social Engineering*

**LOW SEVERITY**

| | |
|---|---|
| Employee Satisfaction | 0 |
| Corporate Email Used on Marketing Sites | 0 |
| Corporate Email Used on Short-Term Lending Sites | 0 |

**POSITIVE SIGNALS**

*There are no Positive Risk Issues to detect for Social Engineering*

**INFORMATIONAL**

| | |
|---|---|
| Leaked Company Emails Open to Spear-Phishing | 0 |

No issues found.