External Network Security Assessment

Wanstor

Version 1.0 – August 25, 2022

Prepared By
Emma Hackett

Prepared For
Dave Ferrans

1 Executive Summary

This report presents the findings of the external infrastructure security assessment conducted on behalf of Wanstor Limited for one of their key clients Shenfield High School. The assessment was conducted on 15/08/2022.

The hosts being assessed were part of the external facing IP ranges that belong to Shenfield High School.

Overview

The security assessment identified a number of issues in relation to the infrastructure within scope. The most significant issues posed a high risk to Shenfield High School. It is recommended that the identified issues are addressed as described within this report in order to ensure that the organisation's information assets are suitably protected. This will, in turn, minimise the risk to which Shenfield High School is exposed.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
External Infrastructure Assessment	0	2	0	4	**6**
Total	**0**	**2**	**0**	**4**	**6**

Assessment Summary

The most significant issues discovered during the assessment related to the use of outdated and unsupported software on two of the assessed hosts. Security vulnerabilities known to be present in the outdated and unsupported version of Outlook Web Access (OWA) present on one host were assessed to pose a high risk. These known issues could allow an appropriately positioned attacker to execute code remotely on the affected host and to abuse missing server-side request forgery protections to perform actions in the context of legitimate users of the OWA software.

The second high risk issue arose because two of the hosts within scope may have been running an outdated and unsupported version of the Microsoft Windows operating system. This version was inferred from the version of an associated software package rather than confirmed directly. Furthermore, it is possible that an extended support service (valid until January 2023) may be in place. Known issues with this version could allow an attacker to execute code remotely, or to escalate their privileges if they gained a low privileged foothold on a host; but it was not possible to confirm or further investigate these issues within the scope of this unauthenticated assessment. However, if this software was unsupported, the hosts would remain vulnerable to any issues published after the standard end of support date (January 2020).

The remaining issues were all assessed to pose a low risk or are reported for information only. Nevertheless, it is recommended that these are reviewed and addressed so as to bring the infrastructure within scope into line with security best practice. It is important to recognise that even low risk issues can be exploited in combination with other issues as part of a wider attack which seeks to compromise an environment or application. In addition, resolving lower risk issues can have the dual benefit of reducing the attractiveness of systems to opportunistic attackers as well as enhancing the overall security posture.

More detailed information on each of the issues which were identified is included in the Technical Details section of this report.

Strategic Recommendations

Much of the risk to which Shenfield High School was exposed was as a result of the use of outdated or unsupported software. It is therefore recommended that, in addition to addressing the individual issues which are set out in this report, the organisation's patching policy and procedures should be reviewed. In particular, it should be ensured that there are processes in place to identify software which is approaching end of life. This should be done sufficiently far ahead of the end of life date that the logistics of software (and any associated hardware) replacement can be handled in an orderly and timely manner. If any unsupported, legacy hosts cannot be upgraded easily, these should be segregated, with additional monitoring put in place to mitigate the exposed risk as much as possible.

Given the security weaknesses which were identified, it is recommended that consideration is given to performing an authenticated security assessment as this could shed light on whether any of the identified issues are exploitable.

In general, it is recommended that the issues set out in this report should be addressed by a structured programme of remedial actions which are prioritised in accordance with the perceived risk to the organisation.

2 Table of Contents

1 Executive Summary 2
2 Table of Contents 4
3 Document Control 5
4 Technical Summary 6
5 Table of Findings 7
6 Risk Ratings 8
7 Finding Details 10
8 Supplemental Data - Tool Output - testssl.sh 22
9 Contact Info 24

3 Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Shenfield High School or Wanstor Limited.

NCC Group gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

Document Data

Data Classification	Client Confidential
Client Name	Wanstor
Project Reference	WANS007
Proposal Reference	O-176503
Document Title	External Network Security Assessment
Author	Emma Hackett

Document History

Version	Issue Date	Issued by	Change Description
0.1	2022-08-11	Emma Hackett	Draft for NCC Group internal review only
0.2	2022-08-22	Tom Kramkowski	Revised QA
1.0		Emma Hackett	Released to client

Document Distribution List

Name	Role
Dave Ferrans	IT Network Manager, Shenfield High School
Emma Hackett	Junior Security Consultant, NCC Group
Lee Kendal	Account Manager, NCC Group

4 Technical Summary

NCC Group was contracted by Wanstor Limited on behalf of one of their key clients, Shenfield High School, to conduct an unauthenticated external infrastructure security assessment of the systems within scope. The aim of the assessment was to identify security issues that could negatively affect Shenfield High School's business or reputation if they led to the compromise or abuse of systems.

Scope

The security assessment was carried out in the live environment and included the following section. The IP addresses within the scope are listed below:

- External infrastructure assessment of the following hosts:
  - 62.252.9.177
  - 62.252.9.178
  - 62.252.9.179
  - 62.252.9.180
  - 62.252.9.181

Caveats

Checks that would have a high probability of causing disruption to the named hosts were excluded. Denial of service attempts were excluded for the same reason.

Post Assessment Cleanup

Revert any WAF/IDS/IPS/firewall changes which were made for the purposes of the assessment.

5 Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

Title	Status	ID	Risk
Unsupported Outlook Web Access (OWA) Email Portal	New	YCX	High
Unsupported Operating System in Use	New	C4D	High
Default IIS Content	New	GJW	Low
Simple Network Management Protocol (SNMP) Externally Facing	New	WMX	Low
Multiple SSL / TLS Cipher Suite Issues	New	XEF	Low
Multiple SSL / TLS Protocol Issues	New	24J	Low

6 Risk Ratings

The table below gives a key to the ratings used throughout this report to provide a clear and concise risk scoring system.

It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Risk Rating	CVSS Score	Explanation
Critical	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
High	7.0 - 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in the short term.
Medium	4.0 - 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved as part of the ongoing security maintenance of the system.
Low	1.0 - 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
Info	0 - 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.

Impact

Impact reflects the effects that successful exploitation has upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

Rating	Description
High	Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.
Medium	Attackers can read or modify some unauthorised data on a system, deny access to that system, or gain significant internal technical information.
Low	Attackers can gain small amounts of unauthorised information or slightly degrade system performance. May have a negative public perception of security.

Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

Rating	Description
High	Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.
Medium	Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.
Low	Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

7 Finding Details

High

Unsupported Outlook Web Access (OWA) Email Portal

Overall Risk	High	**Finding ID**	NCC-WANS007-YCX
Impact	High	**Component**	External Infrastructure Assessment
Exploitability	Medium	**Category**	Patching
		Status	New

Description

An outdated instance of the Outlook Web Access (OWA) portal 14.3.513.0 was in use. This version of OWA is susceptible to publicly disclosed vulnerabilities which include the presence of arbitrary code execution vulnerabilities and missing cross-site request forgery (CSRF) protection. These vulnerabilities could lead to the compromise of sensitive information or of the underlying host.

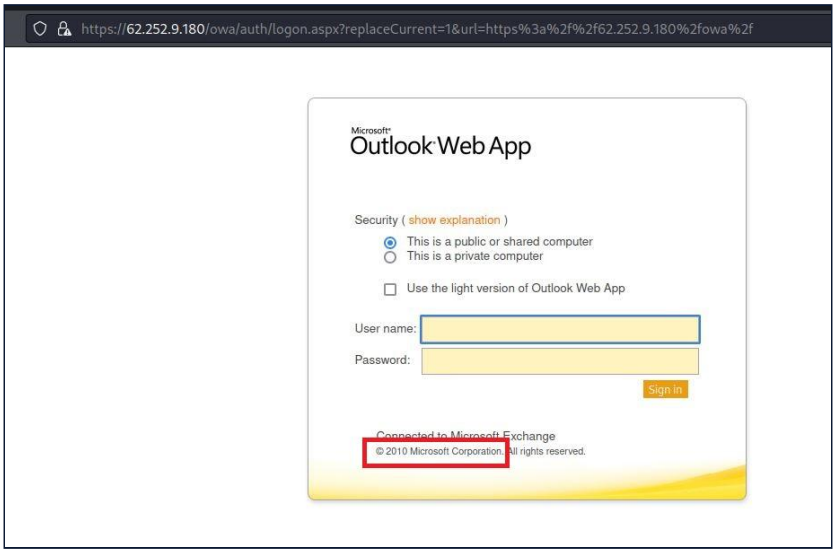

Figure 1: Affected outdated login page found on the host

The version of OWA in use was inferred from the version of Microsoft Exchange Server identified on the affected host, as shown below:

```
The remote host is running Microsoft Exchange Server:

name:    2010 SP3
version: 14.3.513.0
```

This version became unsupported as of 2020-10-13. The presence of this version also indicates that the operating system in use on this server was Windows 2008 R2, which also reached end of life (EoL) January 14, 2020. Refer to finding "Unsupported Operating System in Use" for more information on this.

There will generally be no new security patches for a product after it reaches its EoL. In addition, the vendor is unlikely to investigate or acknowledge reports of vulnerabilities in it. As a result, the web server will remain vulnerable to any issues published after the EoL date and so the exposed risk will tend to increase over time.

As this was an unauthenticated assessment it was not possible to determine what (if any) patches had been applied. In addition, it was not possible to confirm if this host was affected by any publicly available exploits due to the limited time allocated for this assessment. Similarly, no testing of custom exploits was performed for the same time reasons and because this would lead to a risk of server availability problems.

Recommendation

Upgrade the OWA product version to the latest stable and supported version (OWA has been relaunched as Outlook on the web). It is expected that this would also require the upgrading of Exchange Server and the Windows operating system to the latest stable and secure versions in a supported branch released by Microsoft.[1] [2] [3] [4]

Location

- https://62.252.9.180/owa/auth/login.aspx

1. Vulnerability in Outlook Web Access Could Allow Elevation of Privilege (KB2401593): https://docs.microsoft.com/en-us/security-updates/securityadvisories/2010/2401593
2. Supported browsers for Outlook on the web: https://support.microsoft.com/en-us/office/supported-browsers-for-outlook-on-the-web-and-outlook-com-ca350265-6284-4682-9abd-85fc2bd37934
3. Enable Outlook on the Web Using Opt-in Toggle: https://techcommunity.microsoft.com/t5/outlook-blog/an-early-version-of-the-new-outlook-on-the-web-will-be-available/ba-p/225338
4. Exchange Server Supportability Matrix: https://docs.microsoft.com/en-us/exchange/plan-and-deploy/supportability-matrix?view=exchserver-2019

High

Unsupported Operating System in Use

Overall Risk	High	**Finding ID**	NCC-WANS007-C4D
Impact	High	**Component**	External Infrastructure Assessment
Exploitability	Undetermined	**Category**	Patching
		Status	New

Description

The version of Internet Information Services (IIS) running on two hosts was used to infer the version of Windows Server operating system running on these hosts. This was Windows Server 2008 R2, a version which is no longer supported by Microsoft. Based on this issue the Windows server may be susceptible to publicly disclosed vulnerabilities which include, remote code execution (RCE) and privilege escalation.

The version of IIS running on these hosts was disclosed by the the HTTP `Server` response header returned by the hosts. An attacker could also use this information to gain a greater understanding of the underlying technologies involved and tailor further attacks to this specific product.

```
$ curl -I http://62.252.9.181
HTTP/1.1 401 Unauthorized
Content-Length: 0
Server: Microsoft-IIS/7.5
SPRequestGuid: 07c9047d-6154-49bc-9374-8cd93dfdd66b
WWW-Authenticate: NTLM
WWW-Authenticate: Basic realm="62.252.9.181"
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 14.0.0.6029
Date: Mon, 15 Aug 2022 09:11:23 GMT
```

The IIS version was also disclosed on other systems being tested:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 29 Oct 2012 11:10:21 GMT
Accept-Ranges: bytes
ETag: "f36ddfcc5b5cd1:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 15 Aug 2022 14:26:40 GMT
Connection: close
Content-Length: 689
```

Support for this operating system ended in January 2020.[5] Should any new exploits become available for the operating system in use, they would almost certainly not be patched by the vendor, even if they could lead to full system compromise.

Extended Security Updates (ESU) is available for Windows Server 2008 R2 which may cover the server until the 10th of January 2023 (or later for Azure). Due to the limitations of

5. Microsoft Docs - Lifecycle - Windows Server 2008 R2 - https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2008-r2

an unauthenticated infrastructure assessment, it was not possible to determine if the affected server was covered by ESU.

Note it was not possible to confirm if this host was affected by any publicly available exploits due to the limited time allocated for this assessment. Similarly, no testing of custom exploits was performed for the same time reasons and because this would lead to a risk of server availability problems.

Recommendation

Upgrade the affected host to a later, supported version of Windows Server.

The web server should be reconfigured so that software version information is not included in HTTP responses.

Extended support is available in the form of ESU until January 10, 2023.[6] If ESU is not already in place, it is recommended that consideration is given to making use of it until the server can be upgraded.

Location

- http://62.252.9.181
- https://62.252.9.180

6. https://docs.microsoft.com/en-us/windows-server/get-started/extended-security-updates-overview

Low

Default IIS Content

Overall Risk	Low	**Finding ID**	NCC-WANS007-GJW
Impact	Medium	**Component**	External Infrastructure Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

Default IIS content was found at `https://62.252.9.180/`. This takes the form of files and directories which are created during the installation of IIS. This default content should be removed, in order to reduce the opportunity to attack the host (although it is relatively unlikely that any vulnerabilities will be discovered in this content). Furthermore, the presence of this content may allow an attacker to accurately determine the version of web server software in use, providing further justification for its removal.

Note this finding could indicate that server-side content and settings are in a default or unhardened state.

Figure 2: The IIS7 default page is shown hosted at the affected address.

It should also be noted that this default web page shows that IIS7 is in use, this could indicate that the operating system running is Windows 2008 R2 to which is unsupported and reached end of life support on Jan 14, 2020. Refer to finding "Unsupported Operating System in Use" for more information relating to this.

Recommendation

The default content listed above should be removed. In the unlikely event that it serves a legitimate business purpose, it should be renamed to something other than the well-known default values.[7]

7. CIS Microsoft IIS 7 Benchmark, Section 1.1.2: https://www.cisecurity.org/cis-benchmarks/#microsoft_iis

Location

- https://62.252.9.180/

Low

Simple Network Management Protocol (SNMP) Externally Facing

Overall Risk	Low	**Finding ID**	NCC-WANS007-WMX
Impact	Low	**Component**	External Infrastructure Assessment
Exploitability	Low	**Category**	Access Controls
		Status	New

Description

A service which implemented the Simple Network Management Protocol (SNMP) was exposed on a publicly accessible host. SNMP facilitates the exchange of management information between network devices. It was determined that the UDP port 161 was open and could be used to connect to the SNMPv3 service. This is a more secure version than SNMP versions 1 and 2, but v3 is still potentially vulnerable to brute-force attacks.

SNMPv3 will respond to correctly formatted requests and provide some information about itself as part of the reply. Brute-force attacks against the SNMP interface were unsuccessful within the limited time available for this assessment. However, it may be possible that a dedicated attacker with more time available could identify valid usernames for the service and so conduct better targeted, and perhaps more effective, attacks.

The following excerpt from a scan performed by the Nmap tool shows information about the affected service:

```
PORT    STATE SERVICE VERSION
161/udp open  snmp    Cisco SNMP service; ciscoSystems SNMPv3 server
| snmp-info:
|   enterprise: ciscoSystems
|   engineIDFormat: mac
|   engineIDData: 00:18:8b:45:23:e9
|   snmpEngineBoots: 16
|_  snmpEngineTime: 101d02h46m06s
```

Recommendation

Disable the SNMP service on the affected hosts if it does not fulfil a specific business purpose or configure SNMP so that it is restricted to the Local Area Network by configuring firewall filter rules.[8] [9]

Ensure that any user account passwords are complex and strong. Remove the SNMP service from the device if it is not required.

Location

- 62.252.9.177 udp/161

8. CVE-1999-0517 Reference: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0517
9. Securing SNMP: A Look at Net-SNMP (SNMPv3): www.sans.org

Low

Multiple SSL / TLS Cipher Suite Issues

Overall Risk	Low	**Finding ID**	NCC-WANS007-XEF
Impact	Medium	**Component**	External Infrastructure Assessment
Exploitability	Low	**Category**	Cryptography
		Status	New

Description

Security issues were found with the cipher suites offered by the web servers running on two hosts. These issues provide an attacker with a better opportunity to compromise the confidentiality of secure connections used by targeted victims.

The following table summarises the issues found. Links to further relevant information are provided in the footnotes.

Issue	Description	Rating
Weak / Medium Cipher Suites	Keys with an effective length shorter than 128 bits are not secure enough to withstand a brute-force attack. Although Triple DES (3DES) nominally uses a 168 bit key, it has been shown to provide at best an effective key strength of 112 bits, which is less than the recommended 128 bits. It is also vulnerable to the Sweet32 attack as it has a block size of 64 bits.	Low
RC4 Cipher Suites	RC4 has long been known to have a variety of cryptographic weaknesses, which has driven the IETF to release RFC 7465 to discourage the use of RC4 for SSL/ TLS connections. Major browser vendors dropped support for RC4 in default browser configuration in 2016, and all current release versions require manual configuration to enable RC4 support. Please note that although RC4 was not the preferred cipher in use on the affected hosts it was found to be accepted.	Low
Weak Diffie-Hellman Key Exchange (Logjam)	Cipher suites were supported that do not use Diffie-Hellman (DH) parameters of sufficient strength. This could potentially allow an attacker to compromise the confidentiality and integrity of secure connections.	Info
Sweet32	Block ciphers that use 64 bit blocks are affected by a vulnerability known as Sweet32. A man-in-the-middle attacker with sufficient resources can exploit this vulnerability using a ‘birthday’ attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext. This can result in the disclosure of the secret text, which might include the content of secure HTTPS cookies.	Low

The risk rating of the overall issue has been chosen to match the highest listed in the above table.

The following table lists the affected services and the specific issues which affect them:

IP Address	Port	Weak / Medium Cipher Suites	RC4	SWEET32	Weak Diffie-Hellman Key Exchange (Logjam)
62.252.9.179	443	X		X	
62.252.9.180	443	X	X	X	X

Refer to Supplemental Data - Tool Output - testssl.sh for more information relating to this issue.

Recommendation

The following table summarises the recommendations to mitigate the risk from the above findings.[10] [11] [12]

Issue	Recommendation
Weak / Medium Cipher Suites	Disable all ciphers that have an effective key length of less than 128 bits, including 3DES. [13] [14] It is recommended that 3DES should be preferred over RC4. This is because, in the current climate, there is probably greater reputational damage from supporting RC4.
RC4 Cipher Suites	Disable support for RC4 cipher suites. This should be aligned with removing SSLv3 support to avoid exposure to the POODLE attack. [15] [16]
Weak Diffie-Hellman Key Exchange (Logjam)	Update the Diffie-Hellman (DH) configuration to use a 2048 bit prime. Alternatively, use DH cipher suites based on elliptic-curve (EC) cryptography. [17] [18] [19]
Sweet32	Avoid using 64 bit block ciphers such as 3DES. Alternatively, place limitations on the number of requests that are processed over the same TLS connection.[20]

Location

- 62.252.9.179 tcp/443
- 62.252.9.180 tcp/443

10. NCSC - Using TLS to Protect Data: https://www.ncsc.gov.uk/guidance/tls-external-facing-services
11. SSL/TLS Deployment Best Practices by SSL Labs: https://www.ssllabs.com/projects/best-practices/index.html
12. OWASP Transport Layer Protection Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
13. How to Restrict the Use of Certain Cryptographic Algorithms and Protocols by Microsoft: https://support.microsoft.com/default.aspx?scid=kb;en-us;245030
14. A Roster of TLS Cipher Suite Weaknesses by Google: https://googleonlinesecurity.blogspot.co.uk/2013/11/a-roster-of-tls-cipher-suites-weaknesses.html
15. Internet Engineering Task Force (IETF) - Prohibiting RC4 Cipher Suites: https://datatracker.ietf.org/doc/html/rfc7465
16. Royal Holloway Information Security Group Paper: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-garman.pdf
17. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice: https://weakdh.org
18. Guide to Deploying Diffie-Hellman for TLS: https://weakdh.org/sysadmin.html
19. Explanation of Logjam: https://blog.cryptographyengineering.com/2015/05/attack-of-week-logjam.html
20. Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN: https://sweet32.info

Low

Multiple SSL / TLS Protocol Issues

Overall Risk	Low	**Finding ID**	NCC-WANS007-24J
Impact	Medium	**Component**	External Infrastructure Assessment
Exploitability	Low	**Category**	Cryptography
		Status	New

Description

Security issues were found with the protocols offered by the web servers running on two hosts — either in their configuration or in their implementation by virtue of the particular software version running. The potential impact of these issues ranges from denial of service conditions to the opportunity for an attacker to compromise the confidentiality of secure connections used by targeted victims.

The following table summarises the issues found. Links to further relevant information are provided in the footnotes.

Issue	Description	Rating
SSLv2 Supported	SSL version 2 has been deprecated on account of several serious cryptographic flaws.	Low
SSLv3 Supported	SSL version 3 is vulnerable to the POODLE attack, which allows an active man-in-the-middle attacker to try to decrypt short sections of cipher text, providing the victim can be made to issue multiple requests to the site.	Low
POODLE over TLS	The POODLE attack allows an active man-in-the-middle to try to decrypt short sections of cipher text, providing the victim can be made to issue multiple requests to the site. Although originally disclosed as an SSLv3 bug, a TLS service can suffer from the same flaw if it does not adhere strictly to the TLS specification.	Low
TLS Version Support	Although TLS versions considered secure were supported (TLS 1.2). However, the latest version of TLS (1.3) was not offered. Legacy TLS versions no longer considered secure (TLS 1.0, 1.1) were supported.TLS versions 1.2 and 1.3 are more resistant to known attacks than versions 1.0 and 1.1. Version 1.2 and 1.3 support more modern cipher suites that are widely acknowledged to offer the best cryptography available for securing Internet connections. Major browsers now flag TLS v1.0 and TLS v1.1 as insecure.	Low
BEAST	An attacker in a position to sniff network traffic and inject content into a victim's browser may be able to decrypt sensitive traffic in what is known as the BEAST attack. This attack is also dependent on the use of a cipher suite that itself uses a block cipher in CBC mode under SSL or version 1.0 of TLS. However, while there is no fully effective server-side remedy, all major browser vendors have implemented client-side fixes since October 2013.	Info

Issue	Description	Rating
DROWN	DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) exists due to a flaw in the implementation of Secure Sockets Layer Version 2 (SSLv2), and may allow captured TLS traffic to be decrypted.	Low

The risk rating of the overall issue has been chosen to match the highest listed in the above table.

The following table lists the affected services and the specific issues which affect them:

IP Address	Port	POODLE	BEAST	DROWN	SSL v3	SSL v2	TLS 1.0/1.1
62.252.9.179	443		X				X
62.252.9.180	443	X	X	X	X	X	X

Refer to Supplemental Data - Tool Output - testssl.sh for more information relating to this issue.

Recommendation

The following table summarises the recommendations to mitigate the above findings. Where possible, advice on specific software is provided in the footnotes.[21] [22] [23]

Issue	Recommendation
SSLv2 Supported	Disable SSLv2 on the server.[24] [25] [26]
SSLv3 Supported	Disable SSLv3 support but note that old browsers that support SSLv3 as their highest available protocol will no longer be able to connect, e.g. Internet Explorer 6 in its default state.[27] [28] [29]
POODLE over TLS	Consult the vendor for a patch.
TLS Version Support	Ensure that versions 1.2 and 1.3 only are supported.[30] [31] [32] Configure the server to prefer the latest cipher suites that they offer, such as AES-GCM (TLS 1.2 only).

21. NCSC - Using TLS to Protect Data: https://www.ncsc.gov.uk/guidance/tls-external-facing-services
22. SSL/TLS Deployment Best Practices by SSL Labs: https://www.ssllabs.com/projects/best-practices/index.html
23. OWASP Transport Layer Protection Cheat Sheet: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
24. Prohibiting Secure Sockets Layer (SSL) Version 2.0: https://tools.ietf.org/html/rfc6176
25. Apache Directives for SSL: https://httpd.apache.org/docs/current/ssl/ssl_howto.html
26. Disabling SSL 2.0 in Microsoft Internet Information Services: https://support.microsoft.com/kb/187498
27. Analyses of POODLE attack: https://www.imperialviolet.org/2014/10/14/poodle.html,https://blog.cryptographyengineering.com/2014/10/attack-of-week-poodle.html
28. POODLE and TLS: https://www.imperialviolet.org/2014/12/08/poodleagain.html
29. Disabling SSLv3: https://httpd.apache.org/docs/current/ssl/ssl_howto.html, https://support.microsoft.com/kb/187498/en-us, http://nginx.com/blog/nginx-poodle-ssl/
30. Mozilla Server Side TLS: https://wiki.mozilla.org/Security/Server_Side_TLS#Recommended_configurations
31. Google: https://googleonlinesecurity.blogspot.co.uk/2013/11/a-roster-of-tls-cipher-suites-weaknesses.html,https://www.chromium.org/Home/chromium-security/education/tls#TOC-Obsolete-Cipher-Suites
32. Overview of TLS v1.3: https://www.owasp.org/images/9/91/OWASPLondon20180125_TLSv1.3_Andy_Brodie.pdf

Issue	Recommendation
BEAST	There is no definitive server-side remedy beyond supporting TLSv1.3 or TLSv1.2 with TLS_FALLBACK_SCSV, which both rely on compatible browsers to be effective.[33] [34] [35]
DROWN	Disable SSLv2 and export grade cryptography cipher suites (where applicable). Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.[36]

Location

- 62.252.9.179 tcp/443
- 62.252.9.180 tcp/443

33. Original BEAST Attack: https://vnhacker.blogspot.co.uk/2011/09/beast.html
34. SSL Labs: https://community.qualys.com/blogs/securitylabs/2013/09/10/is-beast-still-a-threat,https://community.qualys.com/blogs/securitylabs/2013/10/31/apple-enabled-beast-mitigations-in-os-x-109-mavericks
35. TLS_FALLBACK_SCSV: https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-05,https://www.exploresecurity.com/poodle-and-the-tls_fallback_scsv-remedy/
36. The DROWN Attack: https://drownattack.com/

8 Supplemental Data - Tool Output - testssl.sh

Refer to finding "Multiple SSL / TLS Protocol Issues" and finding "Multiple SSL / TLS Cipher Suite Issues" for more information on the issues identified by `testssl.sh`.

Testing data for host 62.252.9.180

```
Testing cipher categories

SSLv2      offered (NOT ok), also VULNERABLE to DROWN attack -- 2 ciphers
SSLv3      offered (NOT ok)
TLS 1      offered (deprecated)
TLS 1.1    offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol

Testing vulnerabilities

Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
ROBOT                                     not vulnerable (OK)
Secure Renegotiation (RFC 5746)           supported (OK)
Secure Client-Initiated Renegotiation     not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected.  - only supplied "/" tested
                                     Can be ignored for static pages or if no secrets in the page
POODLE, SSL (CVE-2014-3566)               VULNERABLE (NOT ok), uses SSLv3+CBC  (check TLS_FALLBACK_SCSV mitigation below)
TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
FREAK (CVE-2015-0204)                     not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                     Make sure you don't use this certificate elsewhere, see:
                                     https://censys.io/ipv4?q=223318D5549270A47E8FA0D2EBA45B36725650D471F470157E4A70C64AB1EA70
LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                     but no DH EXPORT ciphers
BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                     TLS1: ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES128-SHA AES256-SHA AES128-SHA DES-CBC3-
                                     ↳ SHA                                VULNERABLE -- but also supports higher protocols  TLSv1.1

Supported Server Cipher(s):

Accepted  TLSv1.2  128 bits  RC4-SHA
Accepted  TLSv1.2  128 bits  RC4-MD5
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
```

```
Accepted  TLSv1.1  128 bits  RC4-SHA
Accepted  TLSv1.1  128 bits  RC4-MD5
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5
```

Testing data for host 62.252.9.179

```
Testing cipher categories

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      offered (deprecated)
TLS 1.1    offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol

Testing vulnerabilities:

Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
ROBOT                                     /usr/bin/testssl: line 1926: printf: missing hex digit for \x
Fixme: Conversion of public key failed around line 16811
Secure Renegotiation (RFC 5746)           Not supported / VULNERABLE (NOT ok)
Secure Client-Initiated Renegotiation     not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
BREACH (CVE-2013-3587)                    no HTTP compression (OK)  - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)              Rerun including POODLE SSL check. Downgrade attack prevention NOT
↳ supported                                                                          SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses
↳ 64 bit block ciphers
FREAK (CVE-2015-0204)                     not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no common prime detected
BEAST (CVE-2011-3389)                     TLS1: ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA
                                  AES256-SHA AES128-SHA DHE-RSA-AES256-SHA
                                  DHE-RSA-AES128-SHA DES-CBC3-SHA
                                  VULNERABLE -- but also supports higher protocols  TLSv1.1 TLSv1.2 (likely mitigated)
LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

9 Contact Info

The team from NCC Group has the following primary member:

- Emma Hackett – Junior Security Consultant
  emma.hackett@nccgroup.com

The team from Wanstor has the following primary members:

- Dave Ferrans – Shenfield High School
  D.Ferrans@shenfield.essex.sch.uk
- Harry Sinclair – Wanstor Limited
  Harry.Sinclair@wanstor.com