Cyber Security Penetration Test

Executive Report

Company Business Networks
Q1 2019

Prepared for:
Company Name

NAVISEC

ENGAGEMENT DETAILS

Client's Information	**Company Name** Address Line 1 City, State, Zip https://example.org/
Client's POC	**John Doe,** (123 456 2332 john@example.org
Consultant Information	**NaviSec, LLC** 8404 Benjamin Road Tampa, FL 33634 https://navisec.io/
Consultant's POC	**Joe Bloggs** (123) 456 6034 joe.bloggs@navisec.io

EXECUTIVE SUMMARY

NaviSec, LLC was contracted to perform a security audit for Company Name, Inc. NaviSec gained access to sensitive client data, EMR platform source code, client support systems (such as SFTP), Company Name JIRA, and other critical information and subsystems. Given more time, the potential existed to access company VPN, company email, client LogMeIn resources, Redacted Product, and the backend database server (at a minimum). This report details how the environment was penetrated during this security audit.

Note: Often single weaknesses that are identified does not in itself result in full compromise. Attackers leverage several weaknesses to gain full compromise of target systems. This report contains a section titled "Attack Narrative" that details how multiple weaknesses were leveraged to gain full compromise of the Company Name organization.

There are several critical findings identified during the assessment including the following:

Findings

The following table defines the individuals involved with this assessments completion

Name	Remediation Effort
Public Information Gathering - Patient/Healthcare Provider Data Exposed	Quick
Public Information Gathering - Directory Listing	Quick
Public Information Gathering - Source Code Exposure	Quick
Public Information Gathering - Absolute Server File Paths Exposed	Quick
Severity 5 Vulnerability Discovered - MS15-034	Planned

Name	Remediation Effort
SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	Quick
Ability to Upload any File Type to Server	Planned
Insecure Password Generation	Involved
Sensitive Account Information Disclosure	Involved
Insecure Passwords Identified	Planned

SCOPE

Assets

- 10.10.10.10/8
- example.org

ATTACK NARRATIVE

Passive Reconnaissance

The penetration first began with utilizing reconnaissance techniques. Recon included information gathering from publicly available sources such as search engine spidering, viewing public DNS records, domain registration information, and so on. Several sub domains were discovered that opened many different effective attack vectors. For example, redacted1.example.org, redacted2.example.org, payment.example.org and dev.example.org were all able to be found and tested.

In addition, a personal email address is publicly linked to the Company, Inc organization (redacted@yahoo.com). This information in and of itself is not a weakness, but knowing personal email addresses can assist a hacker in identifying targets for social engineering or phishing campaigns.

From there, several open network services were identified and investigated. Many web applications were discovered running on several of the web hosts. Client portals, software versions, directory listings and many other file types and configuration files are also being indexed in search engines.

The penetration test focused on interesting identified hostnames and the Staging server (https://staging.example.org).

For example:

Resources.example.org – Had many interesting files, software packages that could be read, and source code disclosure.
Payment.example.org – Had many interesting files, software packages that could be read, source code disclosure, absolute path disclosure, and directory listing.
Dev.example.org – Had directory listing, source code of Company Inc's EMR portal exposed, OS disclosure, and appeared to have a NAT allowing internet traffic directly into the Company, Inc network.

Active Reconnaissance

A vulnerability assessment was conducted on the external facing IP addresses in Company, Inc Datacenter. The scan revealed several vulnerabilities related to the use of SSLv3 and TLSv1.0 are present in most of Company, Inc web servers. This could result in failure of PCI or other compliance audits. There was also a Severity 5 vulnerability present that could have resulted in patient information disclosure, denial of service, and remote command execution identified on one of Company, Inc's servers (MS15-034 noted later in this document.)

A web application vulnerability assessment was also conducted that identified several web server header weaknesses. Those weaknesses are also discussed later in this document.

Penetration

While performing a web application vulnerability assessment, several attack vectors were identified inside of Company, Inc's web application platform. The following critical attack vectors were identified the ultimately led to penetration and sensitive information disclosure:

- Ability to upload malicious code without restriction to Company, Inc's webserver.
- Ability to disclose files located on the physical and mapped network drives in Company, Inc's datacenter.
- Ability to view exposed absolute file paths (Such as D:/PHI Data).
- Ability to link names and information on the staging server to real people and facilities.
- Locating sensitive Company, Inc account information on the staging server.

Penetration was ultimately achieved within hours of beginning the web application vulnerability assessment. A file containing sensitive Company, Inc login information was identified on the staging server. This file is in the internal messaging system attached to a message as a .doc file. This file contained several pieces of information that looked like internal company IP addresses, external company URLs and login information. Access to Company, Inc's JIRA system was attained from information located in this file.

Once a login to JIRA was obtained, it allowed access to several critical Company, Inc subsystems such as client SFTP, Company email, VPN, LogMeIn, and several other internal and external accounts. While a full analysis of the sensitive data in JIRA was not completed, enough information was gathered to identify a

critical process flaw that allowed a simulated attacker access to critical company infrastructure and provider/patient data.

FINDINGS

The following findings were made during the assessment.

Name	Remediation Effort
Critical Risk Findings	
Public Information Gathering - Patient/Healthcare Provider Data Exposed	Quick
Public Information Gathering - Directory Listing	Quick
Public Information Gathering - Source Code Exposure	Quick
Public Information Gathering - Absolute Server File Paths Exposed	Quick
Severity 5 Vulnerability Discovered - MS15-034	Planned
SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	Quick
Ability to Upload any File Type to Server	Planned
Insecure Password Generation	Involved
Sensitive Account Information Disclosure	Involved
Insecure Passwords Identified	Planned
High Risk Findings	
Information Gathering - Exposed Subdomains	Quick

Name	Remediation Effort
Moderate Risk Findings	
Information Gathering - Software Versions Exposed	Quick
Clickjacking	Planned
X-XSS-Protection Header is not enabled	Quick
The X-Content-Type-Options header is not set	Planned
SSL/TLS use of weak RC4 cipher	Planned
SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	Quick
Incoming Mail Services Allow Plaintext Credentials	Quick
Outgoing Mail Services Allow Plaintext Credentials	Planned
Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Quick
Low Risk Findings	
Information Gathering - Operating System Disclosure	Quick
Informational Findings	
Information Gathering - Login Page Detection	Quick

CRITICAL FINDINGS

The following are the Critical Findings from the assessment.

Public Information Gathering - Patient/Healthcare Provider Data Exposed	Risk: Critical

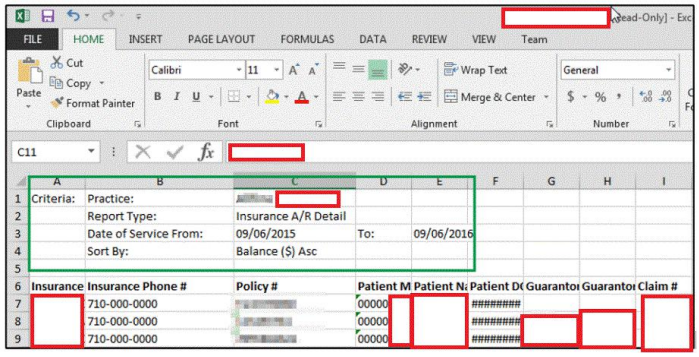
Summary

Company, Inc Product Release Notes potentially exposes client data.

General Attack Information: Malicious actors can use information gathered about your organization to assist in narrowing down effective attack vectors. This information can be benign and result in little potential for additional foothold of an advanced persistent threat or could result in the full compromise of your network. Using public tools it is possible to force the application to leak information by sending messages that reveal the versions and technologies used by the application.

Proof

1) Go to https://www.google.com
2) In the search bar, type "site:example.org ext:pdf"
3) Several Product Release Notes are available. Many of which expose real service provider names and potentially real patient information.
Several examples are available in the Product Release Notes. The following figures are 2 examples (with search engine name correlation).



Remediation

Remove all Product documentation from the site immediately. Develop a process to fully sanitize documentation before it is released to the public. Disable directory indexing in search engines via the robots.txt file.

Affected Hosts

- Evidence affected host A
- Evidence affected host B
- Many other examples available

References

https://www.owasp.org/index.php/Testing:_Spidering_and_googling

Public Information Gathering - Directory Listing	Risk: Critical

Summary

Several servers allow directory listing which could result in source code disclosure, disclosure of sensitive data, software versions, and many other information that may increase the attack surface and increase the risk of a successful attack.

General Attack Information: Malicious actors can use information gathered about your organization to assist in narrowing down effective attack vectors. This information can be benign and result in little potential for additional foothold of an advanced persistent threat or could result in the full compromise of your network. Using public tools it is possible to force the application to leak information by sending messages that reveal the versions and technologies used by the application.

Proof

1) Go to https://www.google.com
2) In the search bar, type 'site:example.org "Parent Directory"'
Other folders on other servers were able to be discovered using publicly available tools. Source code was disclosed on a development server that was identified using DNS Subdomain identification tools. This raised this finding to critical.
Several Directory Listing results are available on several Company, Inc web servers. Some examples follow.

(Redacted Images)

Remediation

Disable directory listing.
Disable search engine indexing for non-marketing web sites.
Create secure Company, Inc default webserver configuration/standardization and deploy to all servers as part of configuration management policy for web servers.

Affected Hosts

Several webservers in Company, Inc's environment are susceptible to this attack. A detailed review of all systems and standardized IIS configuration should be designed and deployed to protect against directory listing.

Some examples:

- http://payment.example.org
- https://resources.example.org

References

1) https://cwe.mitre.org/data/definitions/548.html

Insecure passwords identified	Risk: Critical

Summary

Several "default passwords" were collected throughout the organization that could be used or reused across multiple platforms. Many of which were combinations of the company name with letters, numbers and symbols. Other passwords were a client username encoded in Base64.

Proof

An extensive credential stuffing or brute force campaign was not launched against Company, Inc at this time for several reasons. While some username and password combinations were confirmed across multiple Company, Inc platforms, many others were not tested.

Remediation

Remediation is addressed in the Insecure Password Generation finding.

Affected Hosts

Several Company, Inc Platforms

Some examples:

- http://payment.example.org
- https://resources.example.org

References

None

MODERATE FINDINGS

The following are the Moderate Findings from the assessment.

Information Gathering - Software Versions Exposed	Risk: Moderate

Summary

Certain versions of software are exposing their version information. This may allow an attacker to easily locate already published exploits for certain software versions and gain access to sensitive information.

General Attack Information: Malicious actors can use information gathered about your organization to assist in narrowing down effective attack vectors. This information can be benign and result in little potential for additional foothold of an advanced persistent threat or could result in the full compromise of your network. Using public tools it is possible to force the application to leak information by sending messages that reveal the versions and technologies used by the application.

Proof

1) Go to https://www.google.com
2) In the search bar, type "site:example.org ext:php"

(Redacted proof image)

Remediation

1) Disable search engine indexing of payment.example.org.
2) Disable directory traversal

Affected Hosts

Some examples:

- http://payment.example.org/phpmailer/PHPMailer-FE_v4.11/_lib/default.config.php

References

- https://www.owasp.org/index.php/Testing:_Spidering_and_googling

CONCLUSION

The Company, Inc security infrastructure is currently highly vulnerable to an external attack resulting in compromise of sensitive client and internal company data and gaining elevated privileged access to critical company subsystems. Overall effort of remediation for these weaknesses is high due to some findings being related to business process.

Immediate actions that will result in a strengthened infrastructure are as follows:

- Implementation of a Next Generation Firewall (NGFW) and Web
- Application Firewall (WAF) [In Progress].
- Remediate all High Findings and above as soon as possible.
- Annual cyber security awareness training for all employees. Implementation and enforcement of a Password Policy.
- Implementation and enforcement of a Clean Desk Policy (to include not storing passwords in plaintext saved files on company computers).
- Training of Secure coding standards implemented as part of the Software Development Life Cycle (SDLC).