NetSPI™

3 Attack Surface Mangement (ASM) case studies

that show timely alerting of high-impact vulnerabilities

Introduction

NetSPI Attack Surface Management (ASM) delivered on The NetSPI Platform combines industry-leading technology with our team of proactive security experts to provide comprehensive and continuous monitoring of customers' assets, including identification and validation of exploitable vulnerabilities. Once identified, NetSPI's security experts add context enrichment by manually reviewing each vulnerability to determine its validity, exploitability, and potential impact to customers. The following case studies illustrate the capability NetSPI ASM provides customers who are ready to advance their security program.
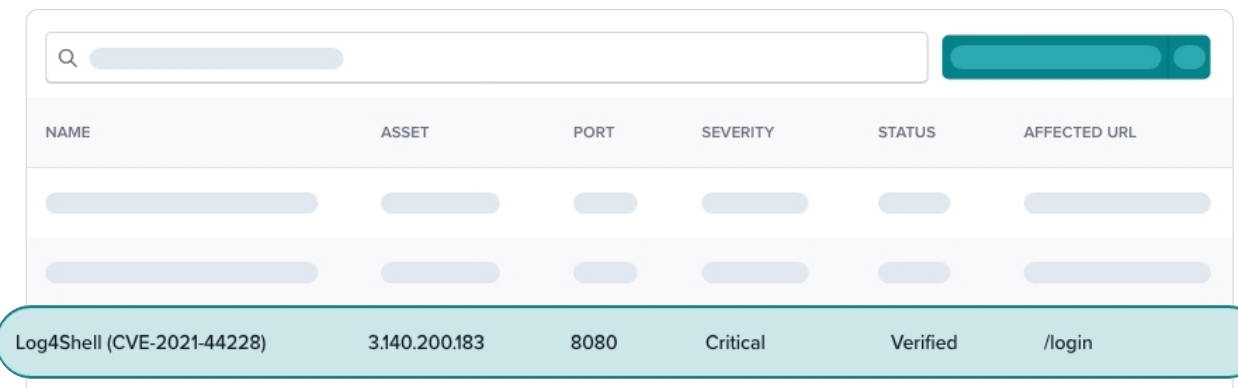
ASM identifies exposed personally identifiable information (PII) for aerospace company

Discovery and impact

Sensitive Information Disclosure vulnerabilities come in many forms, but typically involve the unintentional disclosure of information such as credentials or user data to unauthorized third parties. Except in cases involving disclosure of credentials that might provide access to sensitive systems or networks, information disclosure vulnerabilities often do not pose a direct threat to an organization's infrastructure; however, these vulnerabilities may provide attackers with valuable information about organizations, applications, and business processes with which to plan and execute attacks. Additionally, when attackers gain access to sensitive user data through such vulnerabilities, organizations may experience significant and costly reputational impacts.

In this instance, NetSPI ASM discovered that a web application belonging to one of our customers in the defense and aerospace industry allowed public access to a directory used for storage of files containing user data. With this information, an attacker may have been able to conduct phishing or other social engineering attacks against the organization, potentially leading to breaches of sensitive systems and networks, or damage to the customer's reputation.

NAME	ASSET	PORT	SEVERITY	STATUS	AFFECTED URL
Log4Shell (CVE-2021-44228)	3.140.200.183	8080	Critical	Verified	/login

Process and methodology

1 As part of its web application discovery workflow, NetSPI ASM identified a publicly accessible directory associated with a WordPress plugin, Contact Form 7, which is commonly used to enable file uploads in WordPress applications. Additionally, versions of this plugin are known to contain an Unrestricted File Upload vulnerability (CVE-2020-35489), which could be exploited by an attacker to gain initial access to the application server.

2 As with all potential exposures identified by NetSPI, our security experts were alerted and a manual review was conducted.

3 Upon review of the potential exposure, we determined that the plugin version was not vulnerable to CVE-2020-35489; however, the directory reported by ASM (/wp-content/uploads/wpcf7-submissions) appeared to contain numerous resumes, CVs, and similar documents uploaded by prospective employees.

4 To further assess the impact of this exposure, the team downloaded and reviewed one of these documents and found that it contained PII belonging to a prospective employee.

5 Security experts then documented the vulnerability for sharing with the customer through The NetSPI Platform's built-in reporting mechanism. Because the information disclosure contained sensitive PII, our team assigned the vulnerability a critical severity rating and slated it for immediate delivery, in line with the customer's tailored vulnerability reporting preferences.

Remediation

As part of the vulnerability reporting process, the customer received specific instructions on how to modify the vulnerable application's configuration so that no further sensitive information would be disclosed publicly.
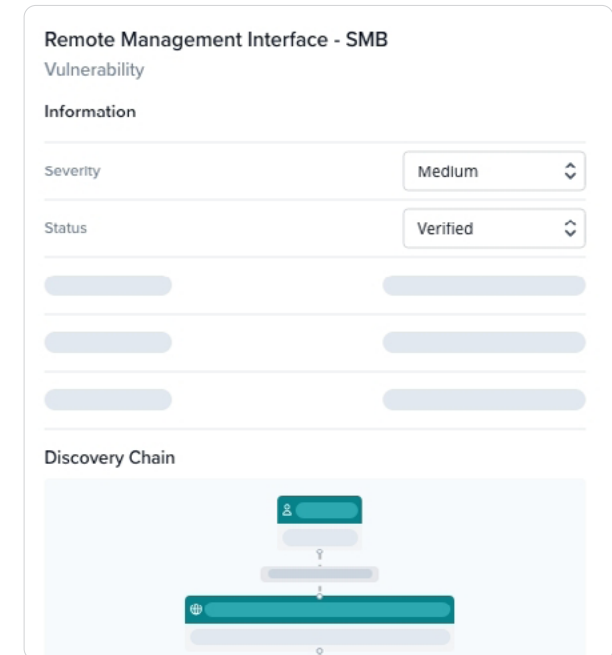
ASM discovers full source code in a healthcare application

Discovery and impact

Sensitive information vulnerabilities do not always pose a direct threat to an organization's infrastructure, but those that do are handled with special urgency. In this instance, the information disclosure discovered by ASM was as bad as they get, exposing the full source code for the application, including configuration credentials and a full database backup containing user data and credentials for users of a healthcare-focused application.

In addition to threatening users' privacy by exposing their personal information to unauthorized parties, this information disclosure also could enable an attacker to take full control over the application's infrastructure, potentially leading to further information disclosures, deployment of ransomware, or any number of costly and damaging attacks.

Process and methodology

1 While scanning for exposures in a customer's web application, NetSPI ASM identified an archive file named for the domain hosting the application (e.g., domain.com.tar.gz) located on the root of the domain. Archive files such as the one identified by NetSPI's Platform are often inadvertently exposed publicly and are frequently found to contain sensitive information pertaining to applications and users.

2 Discovery of the archive file triggered an alert for the NetSPI's ASM security experts, who then performed a manual review of the potential exposure.

3 During this review, the archive was downloaded and extracted, and its contents inspected. Upon inspection, we discovered that the archive contained a backup of the entire web application, including all user data, hashed user passwords, and source code.

4 Though passwords were not being stored in plaintext, hashed passwords can sometimes be recovered to their plaintext form through the process of password cracking. To further assess the impact of the vulnerability, we extracted and successfully cracked a hashed user password from the database backup.

5 Using the cracked password and associated username, we were then able to log into the application, demonstrating that the database backup contained valid data.

6 Given the immediate risk posed to the customer's infrastructure, application, and its users' data, our security experts elevated the original medium severity information disclosure vulnerability to a critical severity rating and immediately reported the vulnerability to the customer, in line with their vulnerability reporting preferences.

Remediation

Though the potential impact of this vulnerability was severe, the fix was simple. Working with the customer, we provided instructions on how to address the root cause of this vulnerability and to prevent similar vulnerabilities from arising in the future.

NetSPI™

ASM alerts to a confirmed subdomain takeover in healthcare

Discovery and impact

Subdomain takeovers are a class of vulnerability that allow attackers to take control of a subdomain by exploiting a misconfiguration. Most users access websites by entering an address (e.g., asm.netspi.com), into a browser. This address is then translated into a more machine-usable format (an IP address) via the Domain Name System (DNS), which tells a user's computer where exactly the website is located on the internet. At a minimum, addresses include a domain (e.g., asm.netspi.com), but may also include a subdomain (e.g., asm.netspi.com), the combination of which tells DNS what specific website a user is trying to access.

A subdomain takeover vulnerability occurs when a DNS record for a subdomain (e.g., a CNAME record) is misconfigured so that it directs a user's browser to an external location or application on the internet that is not directly controlled or managed by the website's owner. If an attacker can control the external location, for example, by registering an account with the external application, then visitors to that subdomain will be directed to the attacker-controlled site and its content. Though the specifics of each subdomain takeover vulnerability can vary greatly, they all enable direct attacks against visitors to a vulnerable subdomain such as theft of credentials or user data, or malware infection.

Process and methodology

1 The NetSPI Platform alerted our ASM security experts to a potential subdomain takeover vulnerability in a website belonging to one of NetSPI's customers in the healthcare industry.

2 Our security experts reviewed the vulnerability details, including the suspected vulnerable subdomain.

3 Upon navigating to the affected subdomain, the team observed that the subdomain was indeed configured to redirect visitors to an external application used for building websites.

4 By examining the DNS records associated with the subdomain and the external application, the security experts were able to identify a way of exploiting this vulnerability by registering an account with the external application.

5 To demonstrate exploitability (an important step NetSPI takes to ensure our customers are not inundated with false positives), and to prevent exploitation of this vulnerability by real-world attackers, security experts registered the necessary account with the external application, documented the process, then reported the vulnerability to the customer in line with their vulnerability reporting preferences.

Remediation

Proactive security experts were able to provide a temporary fix to this vulnerability by registering an account with the external application; however, the root cause of the problem required modifying the customer's DNS records. The customer received specific instructions on what DNS records to modify, as well as general instructions on how to prevent similar vulnerabilities from occurring in the future.
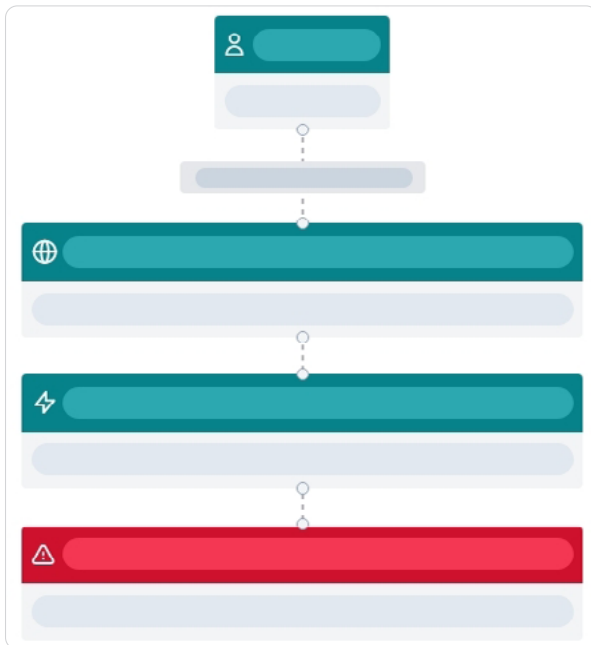
See NetSPI ASM in action
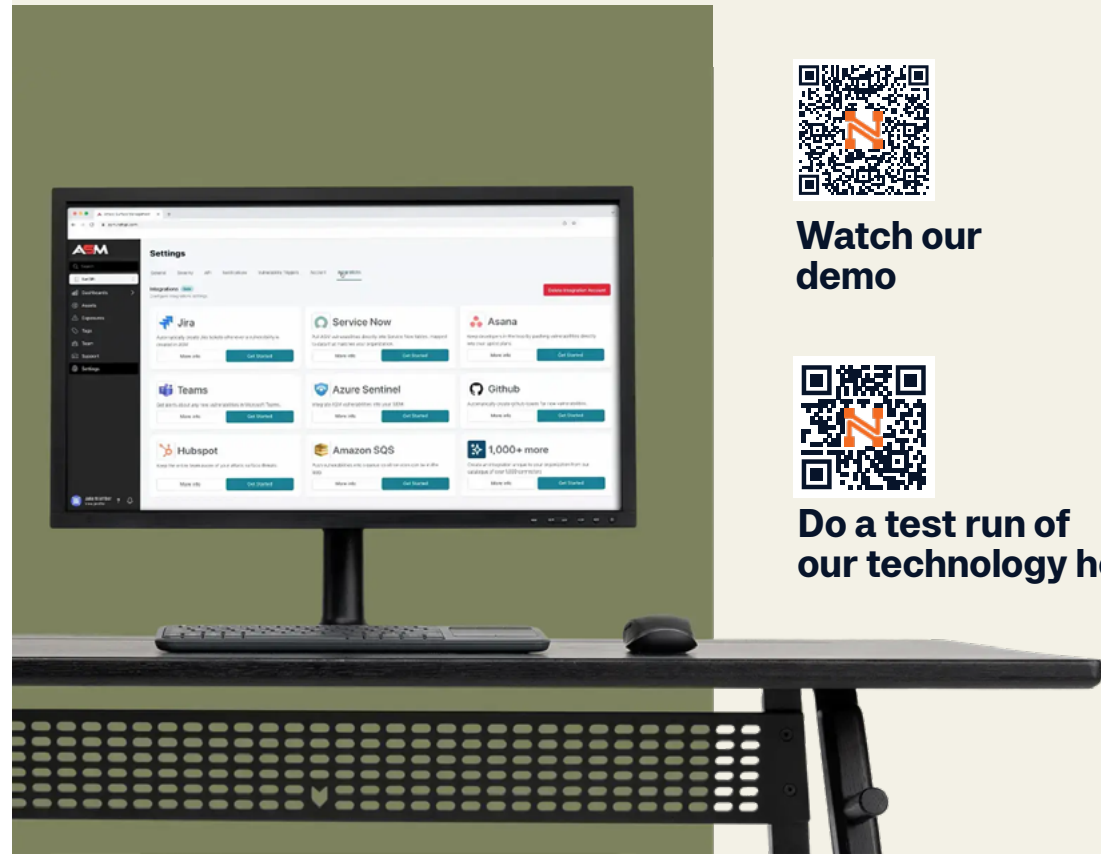
Watch our demo

Do a test run of our technology here

You deserve The NetSPI Advantage

**250+ In-house
security experts**

**Intelligent
process**

**Advanced
technology**

Your proactive security partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), Attack Surface Management (ASM), and Breach and Attack Simulation (BAS).