VERACODE

BIGGEST DATA BREACHES

OF 2020

US Small Business Administration

8,000

BUSINESS OWNERS' DATA EXPOSED

In April of 2020, the United States Small Business Administration (SBA) acknowledged that data of nearly 8,000 business owners may have been exposed to threat actors accessing their Economic Injury Disaster Loan Emergency (EIDL) program online.

While it wasn't clear exactly what caused the flaw, simply hitting the "back" button while in the loan application portal may have shown users sensitive information belonging to other applicants. Though it was possibly caused by a combination of redirects and access-control misconfigurations, the SBA acted quickly and immediately disabled the impacted portion of their website to begin remediating the bug.

THREAT: Cross-Site Scripting

LEARN MORE: Prevention and Remediation

Sensitive information exposure, like we saw with the SBA, is a serious issue that can come from very risky flaws. In 2020, a group called Magecart Group 8 targeted blender manufacturer Nutribullet by inserting a JavaScript web skimmer code onto the company's website. The code targeted Nutribullet's checkout page and was able to capture sensitive payment information from customers. Similar vulnerabilities, such as cross-site scripting (XSS) flaws, enable threat actors to inject client-side scripts into applications for hijacking user accounts, spreading worms and Trojans, controlling browsers remotely, and more.

Nintendo

160,000

USERS EXPOSED

Nintendo announced in April of 2020 that gamers were reporting suspicious activity on their accounts, which led to the discovery of threat actors abusing the Nintendo Network ID (NNID) legacy login system. According to Nintendo, attackers may have accessed nicknames, dates of birth, email addresses, and locations by country for up to 160,000 user accounts.

While Nintendo didn't directly disclose a cause or a source, this breach was most likely the result of credentials stuffing or unsecured points of access that attackers exploited to gain side-door entry into Nintendo's systems.

THREAT: Credentials Management Attack

LEARN MORE: Secure Coding Best Practices

Some experts believe the Nintendo hack may have been made possible by a credential stuffing campaign using previously-stolen data. You can prevent most flaws and vulnerabilities that lead to stolen data with secure coding practices and other careful measures around credentials management. Do not store passwords in easy access locations, use plaintext in software, or forgo encryption. Encryption is crucial, especially for outbound authentication. Limit permissions only to users who need access, limit key functions to the system console, and implement strong protections for encryption keys and files.

Microsoft

250,000,000

CUSTOMER SERVICE + SUPPORT RECORDS EXPOSED

2020 was off to a rough start for Microsoft when it announced a breach of 250 million customer service and support records dating back to 2005. The records included chat transcripts between support and customers, scrubbed from customer service records before they were put into storage. The stolen data contained emails and IP addresses in plain text, but also may have included case numbers and confidential notes.

According to Microsoft, the breach occurred due to misconfigured security rules in an internal database and exposed the records for most of December.

Wattpad

270,000,000

PERSONAL RECORDS EXPOSED

Wattpad, a social storytelling platform, suffered a breach in July of 2020 that exposed more than 270 million records. Impacted data included sensitive information like usernames, passwords, dates of birth, email addresses, IP addresses, and even social media profiles. The leaked SQL database contained over 268 million unique email addresses once duplicates were removed, including over 2 million military addresses and about 140,000 .gov addresses.

Although Wattpad later disclosed that passwords exposed by the breach were salted and cryptographically hashed and that no financial information was stolen, the company announced that it would bolster its password requirements for all user accounts.

THREAT: Cryptographic Flaws

LEARN MORE: Prevention and Remediation

Cryptographic flaws plague many applications due to the notoriously difficult implementation of proper encryption. Salted and hashed passwords — like we saw in the Wattpad breach — are a first line of defense against insecure crypto. Still, issues can arise with broken crypto algorithms, improperly validated certificates, and inadequate encryption strength. While most major languages inherently support good cryptographic practices, such vulnerabilities are preventable with secure coding best practices.

Broadvoice

350,000,000

CUSTOMER RECORDS EXPOSED

In October of 2020, VoIP provider Broadvoice disclosed a leak that involved over 350 million customer records in 10 databases. Names, phone numbers, and call transcripts — including voicemails for medical facilities and financial services companies — were included in the breach, which the company's CEO said was due to an unsecured database.

Though Broadvoice worked quickly to patch the vulnerability, experts warned that the leaked customer records may help facilitate a sophisticated phishing campaign using the personally identifiable information within.

Keepnet Labs

5,000,000,000

RECORDS EXPOSED

Email security company Keepnet Labs was the subject of a data leak that contained over 5 billion records from previous cybersecurity incidents. According to security researchers, sensitive information was robust and organized and included hash types, passwords, leak years, email addresses, email domains, and leak sources. The database was exposed on an unprotected Elasticsearch server while being moved to another server, according to the company, with the firewall disabled for roughly ten minutes.

Although Keepnet Labs took the database offline within an hour once notified, the cache of information was a potential treasure trove for criminals to use in social engineering and phishing attacks.

THREAT: Directory Traversal Exploits

LEARN MORE: Prevention and Remediation

Unsecured servers in instances like the Keepnet Labs data leak can lead to directory traversal exploits. These exploits are used by threat actors to gain unauthorized access to restricted directories and files, which can compromise an entire web server. To prevent directory traversals, developers should make sure that they properly validate user input from browsers, use filters to block certain user input, and keep web server software up to date with current patches — which often contain security fixes.

Data from *State of Software Security* v11

The data reveals that information leakage, CRLF injection, cryptographic issues, and code quality are the most common security vulnerabilities plaguing applications today. Fortunately, we know that through secure coding best practices, educational training, and the right combination of testing tools and integrations, developers are able to write more secure code from the start — which means producing innovative applications that avoid cyberattacks and reduce the risk of costly breaches.

LEARN MORE

veracode.com/SOSS