



 WHITEPAPER

The Top 25+ Source Code Leaks

2020-2024

Table of Contents

Introduction	03
What Is a Source Code Leak?	03
How Is Source Code Leaked?	04
The Impact of a Source Code Leak	04
Source Code Leaks for 2020 to 2024	05
Binance Mercedes-Benz	06
Rockstar Games Ubisoft	07
Samsung Twitter	08
GoDaddy Slack	09
Intel Uber	10
LastPass Globant	11
NVIDIA Nissan	12
Microsoft Intel	13
Capcom Embraer	14
Github Microsoft	15
Nintendo Electronic Arts	16
State of NY, Office of IT Services Daimler	17
US Government Clearview AI	18
Rogers Communications	19
How to Stop Source Code Leaks	20
How Cycode Helps	21
Peace of Mind	23

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

Introduction

The Top 25+ Source Code Leaks, 2020-2024

Source code is the core of any software company's intellectual property. Accessing it is akin to learning the formula to Coca Cola, Kentucky Fried Chicken's 51 herbs and spices, or the architectural drawings for Lockheed's F22 Raptor.

Proprietary source code exposure is a big deal for any software company. It can lead to loss of trust, loss of revenue, and huge fines should sensitive data be exposed. Source code leaks even present safety issues, like when leaked code gives access to a car's onboard systems, allowing attackers to remotely control steering, braking, and other critical functions.

In this report, we explore how source code is leaked and the impact of a leak. Then we share five year's worth of real-world examples to illustrate the far-reaching consequences for businesses, their customers, and their consumers.

What Is a Source Code Leak?

A source code leak is any event that publicly exposes application or operating system code outside of the company that owns it. Source code leaks are dangerous because they can expose vulnerabilities in the design or coding of an application, give away trade secrets, and potentially wreak havoc on software and systems.

Source code often contains hardcoded secrets. This allows attackers to login to critical systems using authentic credentials, which makes it harder for security teams to detect malicious behavior.

Unfortunately for security teams, source code leaks are becoming increasingly common.

From January to June 2023, GitHub received [1,086 takedown notices](#) to remove proprietary code from their platform. This resulted in 14,159 unique projects being taken down from GitHub.

How Is Source Code Leaked?

Broadly speaking, there are three ways in which source code can be leaked:

Attacks: To gain access to source code, hackers may exploit existing software vulnerabilities, leverage compromised credentials, carry out social engineering attacks, or use malware to compromise infrastructure.

Insider threats: Whether it be for personal gain, revenge, or to benefit a competitor, insiders with access to source code may intentionally leak it.

Human error: Tool misconfigurations, lost or stolen devices, and email mistakes can all lead to unauthorized access to source code and subsequent leaks. Even accidentally [sharing sensitive information via ChatGPT](#) can lead to a source code leak.

The Impact of a Source Code Leak

According to the Commission on the Theft of American Intellectual Property, the total value of stolen trade secrets from the US alone is anywhere from \$180 billion to \$540 billion per year.

The impact of a source code leak varies depending on the nature of the code, the context in which it's used, and the organization or project involved. Nonetheless, organizations experience a number of significant consequences:

- ⦿ Loss of intellectual property
- ⦿ Reputational and brand damage
- ⦿ Revenue loss
- ⦿ Regulatory compliance fines
- ⦿ Exposed secrets
- ⦿ Compromised customers
- ⦿ Zero-day exploits

The bottom line: It's essential that organizations keep their code secure.

In the next section, we share 27 real-world examples of source code leaks from 2020 to 2024. Following that, we provide tips on how to prevent source code leaks and how a complete ASPM platform can secure your applications.

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Source Code Leaks
for 2020 to 2024

Date	Organization	Cause
January 2024	Binance	Unknown
January 2024	Mercedes Benz	Compromised credentials
December 2023	Rockstar Games	Compromised credentials
August 2023	Ubisoft	Unknown
May 2023	Samsung	ChatGPT (human error)
March 2023	Twitter	Insider threat
February 2023	GoDaddy	Compromised credentials
December 2022	Slack	Compromised credentials
October 2022	Intel	Unknown
September 2022	Uber	Compromised credentials
August 2022	LastPass	Compromised credentials
March 2022	Globant	System compromise
March 2022	NVIDIA	Ransomware
January 2021	Nissan	Git repository misconfiguration
December 2020	Microsoft	Supply chain attack (Solarwinds)
December 2020	Intel	Ransomware
November 2020	Capcom	Ransomware
November 2020	Embraer	Ransomware
November 2020	GitHub	Accidental commit to GitHub's DMCA section
September 2020	Microsoft	Unknown
July 2020	Nintendo	Compromised credentials
June 2020	Electronic Arts	Unspecified network intrusion
June 2020	State of NY IT Office	Git repository misconfiguration
May 2020	Daimler	Git repository misconfiguration
April 2020	Multiple US Federal Agencies	Misconfiguration (SonarQube)
April 2020	Clearview AI	Repository misconfiguration
January 2020	Rogers Communications	Git repository misconfiguration

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

● **Binance**

● **Mercedes-Benz**

○ Rockstar Games

○ Ubisoft

○ Samsung

○ Twitter

○ GoDaddy

○ Slack

○ Intel

○ Uber

○ LastPass

○ Globant

○ NVIDIA

○ Nissan

○ Microsoft

○ Intel

○ Capcom

○ Embraer

○ Github

○ Microsoft

○ Nintendo

○ Electronic Arts

○ State of NY, Office of IT Services

○ Daimler

○ US Government

○ Clearview AI

○ Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Binance

January 2024

Binance had a “highly sensitive cache of code, infrastructure diagrams, internal passwords” and other technical data posted on a GitHub repository for several months. The leaked code contained passwords for production systems, including several for active AWS servers. Binance claims that the code is outdated and poses “negligible risk” to its end users, though in its GitHub takedown request, the company said the code was posted without permission and represents a “significant risk.” Binance has not disclosed whether the leak was a result of a malicious attack or if an employee accidentally uploaded it to a public repo.

Further Reading:

[GitHub repository exposed Binance’s internal passwords and code](#)

Mercedes-Benz

January 2024

A Mercedes-Benz employee’s authentication token was found in a public GitHub repository during a internet scan by a third party. The GitHub token gave unrestricted access to the company’s source code hosted on an internal GitHub Enterprise Server. It had been exposed since late September 2023. When the exposure was disclosed in January 2024, Mercedes-Benz revoked the API token in question and immediately removed the public repository. A Mercedes-Benz spokesperson said the cause of the leak was “human error.”

Further Reading:

[How a mistakenly published password exposed Mercedes-Benz source code](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- **Rockstar Games**
- **Ubisoft**
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymore Helps

Peace of Mind

The Top 25+ Source Code Leaks

Rockstar Games

December 2023

A year after the LAPSUS\$ hacker group infiltrated Rockstar games, the source code for Grand Theft Auto was leaked online in several places, including on Discord. LAPSUS\$ used social engineering, phishing, MFA fatigue, and SIM swapping to gain access to numerous large organizations' networks, many of which you'll read about further on this list. In August 2023, two members of LAPSUS\$ were tried and convicted for multiple hacking attacks. Since then, LAPSUS\$ has not been very active, though several members are now believed to be part of a new hacking collective.

Further Reading:

[GTA 5 source code reportedly leaked online a year after Rockstar hack](#)

Ubisoft

August 2023

The incident involving Far Cry wasn't a malicious hack. It seems instead to be a curious case of unintended release, but nonetheless underscores the inherent value of source code and the short- and long-term consequences of a leak.

What was exposed but the mysterious uploader? The inner workings of the entire game and engine, including everything from AI behavior to map design, appeared on the Internet Archive in June 2023. Mods for the original Far Cry surged in popularity, but the future security of the game (and others that are leaked) has become an important talking point.

Note that this isn't the first source code leak to happen within the gaming industry. Private repositories for [Watch Dogs: Legion](#) and [League of Legends](#) were also released in 2023.

Further Reading:

[Far Cry's Source Code Has Leaked All Over The Internet](#)

[The original Far Cry's source code has been leaked, uploaded online](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- **Samsung**
- **Twitter**
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Samsung

May 2023

Eager to experiment, Samsung engineers in the semiconductor division used ChatGPT. Samsung shared source code for equipment testing programs and chip testing sequences, along with internal meeting notes containing valuable trade secrets. As a result, OpenAI, ChatGPT's developer, has access to the sensitive data, which raises concerns about intellectual property theft, unfair advantage, and best practice for using AI tools, especially when sensitive information is involved.

Further Reading:

[Samsung workers made a major error by using ChatGPT](#)

Twitter

March 2023

Between January and March 2023, a GitHub user named "FreeSpeechEnthusiast" uploaded snippets of Twitter's internal code, revealing parts of Twitter's recommendation algorithms, moderation tools, and internal APIs. This information could potentially allow attackers to understand how Twitter operates and exploit vulnerabilities for spam, manipulation, or even identity theft.

While Twitter quickly removed the leaked code from GitHub, the leak could complicate Twitter's future development plans and leave it more vulnerable to future hacking attempts. Worse still, it's unclear how the code was obtained in the first place, although employee negligence or a phishing attack are suspected possibilities.

Further Reading:

[Twitter Says Parts of Its Source Code Were Leaked Online](#)

[GitHub takes down repository containing Twitter's source code](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- **GoDaddy**
- **Slack**
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks

GoDaddy

February 2023

A multiyear infiltration came to a head in early 2023 after malicious actors broke into GoDaddy's cPanel shared hosting servers, stole source code, and installed malware targeting websites for phishing and malware distribution. Not only did the stolen code give attackers potential footholds and insights into GoDaddy's inner workings, but, because the breach was discovered by customer reports that their sites were being used to redirect to random domains, the incident has caused reputational damage and impacted customer trust.

Further Reading:

[GoDaddy: Hackers stole source code, installed malware in multi-year breach](#)
[GoDaddy Announces Source Code Stolen and Malware Installed in Breach](#)

Slack

December 2022

Just before the new year, Slack disclosed a security incident involving the theft of some of its private source code repositories. While the details remain somewhat murky, we know that attackers gained access to a limited number of Slack employee tokens, likely through phishing or other social engineering tactics. These tokens were then used to access Slack's externally hosted GitHub repository, where the private code was stored.

The stolen repositories contained internal code and development tools. They also could have given attackers insights into Slack's internal workings and vulnerabilities, making them more vulnerable to future attacks.

Further Reading:

[Slack Says Hackers Stole Private Source Code Repositories - SecurityWeek](#)
[Slack Security Update](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymcode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Intel

October 2022

Although it's unclear who is responsible or how they gained access, Intel's proprietary BIOS/UEFI code was leaked by a third-party and posted on 4chan and Github in a repository named 'ICE_TEA_BIOS.' In total, the repository contained 5.97 GB of files, source code, private keys, change logs, and compilation tools.

Because the leak relates to Intel's 12th generation Intel Core processors, exposed data could make it easier for cybercriminals to discover vulnerabilities and launch zero-day attacks in the product.

Further Reading:

[Intel's source code leaked: Why the breach is a security concern](#)

[Intel confirms leaked Alder Lake BIOS Source Code is authentic](#)

Uber

September 2022

LAPSUS\$ gained access to Uber's internal systems using stolen employee credentials that were purchased from the dark web. After successfully connecting to Uber's intranet, the hacker gained full admin access to the company's VPN and other sensitive services like DA, DUO, Onelogin, AWS, and GSuite.

The attackers got their hands on a vast amount of information, including the source code for Uber's backend systems, critical algorithms like driver-rider matching, and internal communications. They also allegedly accessed Uber's bug bounty reports, which usually contain details of security vulnerabilities yet to be remediated.

While user data remained secure, the leak exposed Uber's technical infrastructure and potentially vulnerable areas, causing significant reputational damage and security concerns.

Further Reading:

[Uber hacked, internal systems breached and vulnerability reports stolen](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- **LastPass**
- **Globant**
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cyscale Helps

Peace of Mind

The Top 25+ Source Code Leaks

LastPass

August 2022

LastPass first reported a hack in August 2022 after attackers accessed their development environment to gain access to portions of their source code and proprietary technical information. The attackers then used this information to launch a series of attacks, including one targeted at a senior DevOps engineer with high-level security authentication.

Over the course of several months, the malicious actors exploited a vulnerability in the engineer's third-party media software package on his home computer, gained access for remote code execution, and installed keylogger malware. Eventually, they stole the engineer's master password, and gained access to encrypted secure notes and decryption keys, which opened the door to critical database backups.

Further Reading:

[LastPass breach: Hackers put malware on engineer's home computer to steal their password | ZDNET](#)

[Last Pass: Notice of Recent Security Incident](#)

Globant

March 2022

IT and software consultancy giant Globant confirmed a breach by the LAPSUS\$ data extortion group who gained unauthorized access to a section of its code repository.

While the breach affected only a "limited" number of customers, the 70GB archive that was released contained source code folders related to Abbott, Facebook, and DHL. It also contained administrator credentials for platforms like Jira, Confluence, GitHub, and Crucible. SOS Intelligence indicates that the leak contained code repositories with private keys (full chain, web server SSL certificates, Globant server, API keys), and over 150 SQL database files.

Further Reading:

[CSRB Exposes Lapsus\\$ Hacker Group's Cyber Extortion Activities and Systemic Failures Enabling Them](#)

[Globant admits to data breach after Lapsus\\$ releases source code](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- **NVIDIA**
- **Nissan**
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks

NVIDIA

March 2022

LAPSUS\$ breached NVIDIA, an American chipmaking company. LAPSUS\$ gained access to sensitive data, including source code related to its popular Deep Learning Super Sampling (DLSS) technology, email addresses and NTLM password hashes for 71,335 employees (which were cracked and shared on various hacking forums), and schematics and source code for drivers and firmware.

Though LAPSUS\$ only initially released 20GB of data, they claimed to have stolen 1TB of NVIDIA's "most closely-guarded secrets" and threatened to publish everything unless the chipmaker complied with their various demands.

Further Reading:

[Hackers Who Broke Into NVIDIA's Network Leak DLSS Source Code Online](#)
[Nvidia's DLSS source code leaked by hackers](#)

Nissan

January 2021

The Nissan leak involved a misconfigured Git server that was left directly accessible to the internet using the default username and password combination of admin/admin. The source code exposed in this incident included Nissan NA mobile apps, the Dealer Business Systems/ Dealer Portal, vehicle connected service, some parts of the Nissan ASIST diagnostics tool, and Nissan/Infiniti NCAR/ICAR services. Leaked source code for anything that connects to a car's onboard systems, like diagnostics tools or services like NCAR, is particularly dangerous. The Jeep Cherokee Hacks of 2015 demonstrated that, with access to onboard systems, hackers may be able to remotely control steering, braking, and other critical functions.

Further Reading:

[Nissan source code leaked online after Git repo misconfiguration](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- **Microsoft**
- **Intel**
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Microsoft

December 2020

Microsoft announced that the hackers behind SolarWinds had accessed Microsoft's internal networks and downloaded source code from repositories containing small subsets of components of its Azure cloud computing service, Intune mobile device management solution, and Exchange business email and calendaring service.

The attackers gained access to the repositories using malware inserted into the Orion IT monitoring platform. Microsoft reported that the attackers appeared to be searching for secrets in the source code, but did not succeed in either finding secrets or using Microsoft's systems to attack others. This is indeed fortunate, considering the number of customers using Azure, Intune, and Exchange who might have been affected had the hackers succeeded. Microsoft said that their development policy prohibits secrets in code, and the investigation confirmed that the code in the affected repositories did not contain any live production credentials. While Microsoft's code leak was limited to the hackers responsible, as opposed to the entire internet, it still qualifies as one of the top leaks due to the widespread distribution of their solutions.

Further Reading:

[SolarWinds hackers accessed Microsoft source code](#)
[Microsoft Internal Solorigate Investigation – Final Update](#)

Intel

December 2020

Habana Labs, an Intel-owned developer of AI processor chips, lost data during a December 2020 cyber attack. Habana builds processors that improve scalability and throughput for AI workloads. Hackers were able to exfiltrate Windows domain account information, DNS zone information for the domain, and the entirety of the company's Gerrit code collaboration tool server using the Pay2Key ransomware software. The hackers responsible then went on to leak images of the Habana Labs source code while making further demands for ransom.

Further Reading:

[Intel's Habana Labs hacked by Pay2Key ransomware, data stolen](#)
[Ransomware masterminds claim to have nabbed 53GB of data from Intel's Habana Labs](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- **Capcom**
- **Embraer**
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Capcom

November 2020

Video game developer Capcom suffered a data leak in November that exposed source code for several top-selling Capcom games, including The Misadventures of Tron Bonne, Resident Evil: The Umbrella Chronicles, a blockbuster game that shipped nearly a million units, and Devil May Cry 2, a top-selling game that shipped 1.7 million units. A ransomware group leaked the source code along with release schedules and corporate financial records. Capcom confirmed the attack and disclosed that some customer information had also been compromised.

Further Reading:

[Resident Evil Village launch date leaked in massive Capcom ransomware attack 3rd Update Regarding Data Security Incident Due to Unauthorized Access](#)

Embraer

November 2020

Source code from Brazilian airplane maker Embraer was leaked in November 2020 following a ransomware attack. Embraer chose to restore its systems from backups rather than pay the ransom. In response, the hackers leaked a set of Embraer files, including embedded systems source code typically used to design and integrate mission-critical systems and secure data channel communications in the aerospace industry. According to Embraer, the incident only caused a temporary impact on operations.

Further Reading:

[Hackers leak data from Embraer, world's third-largest airplane maker](#)
[Embraer S.A.: Material Fact](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- **Github**
- **Microsoft**
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymcode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Github

November 2020

An unknown user posted source code for GitHub Enterprise Server on GitHub's DMCA takedown notices repository. GitHub Enterprise Server is a version of GitHub Enterprise that companies can run on their own on-premises servers to store and manage sensitive code locally.

GitHub Enterprise is not open source, but GitHub routinely ships stripped-down, obfuscated source code to Enterprise Server clients. According to GitHub's CEO, the code dumped to the DMCA repository was a complete, non-obfuscated version of the source code that GitHub had accidentally supplied to a few Enterprise Server customers several months earlier. While there was no sign of malicious doing, the fact is that GitHub's code was exposed to the internet in an unintended fashion, and that qualifies as a leak.

Further Reading:

[GitHub's source code was leaked on GitHub last night... sort of](#)
[GitHub denies getting hacked](#)

Microsoft

September 2020

Microsoft has the unfortunate distinction of appearing on this list multiple times. In September 2020, source code for several Microsoft operating systems was leaked to 4chan. It's not clear how the code was obtained. The code bases leaked included Windows XP, Windows Server 2003, Windows 2000, Embedded (CE 3, CE 4, CE 5, CE, 7), Windows NT (3.5 and 4), and MS-DOS (3.30 and 6.0). The leaked code-bases are not complete. Initially it was unclear whether the code was real, however, the code was compiled and ultimately proven authentic. While these operating systems are older, they still run on a significant number of systems. For example, Windows XP still maintained a nearly 1% market share at the time of the leak in 2020.

Further Reading:

[Windows XP leak confirmed after user compiles the leaked code into a working OS](#)
[Security News This Week: Windows XP Source Code Got Leaked All Over the Internet](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- **Nintendo**
- **Electronic Arts**
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymode Helps

Peace of Mind

The Top 25+ Source Code Leaks

Nintendo

July 2020

Nintendo experienced several major leaks over the course of just a few months. In May 2020, source code was leaked for a “significant number” of games and for the Nintendo Wii console itself. This occurred when servers managed by design partner BroadOn were compromised.

Then in July 2020, source code for a number of games including Super Mario Kart and The Legend of Zelda: A Link to the Past was leaked on 4chan in /v/, a video game forum. This leak was titled “Gigaleak” because it was 3 gigabytes in size. The leak was likely a result of compromised credentials.

Further Reading:

[Massive Nintendo Gigaleak Exposes Source Code Of Classic Games And Consoles On 4Chan](#)
[Nintendo Suffers Another Substantial Leak As Mountains Of Source Code Hit The Web](#)

Electronic Arts

June 2020

An unspecified network intrusion allowed hackers to access more than 780 GB of source code for popular EA games like FIFA '21 and tools like the Frostbite game engine. The Frostbite game engine is used by FIFA, Madden, Battlefield, Star Wars: Squadrons and Anthem. After EA ignored hackers' repeated attempts to obtain ransom payment in exchange for the source code, they leaked the files onto the internet. This was one of the largest troves of gaming source code to ever be leaked publicly on the internet.

Further Reading:

[Hackers Stole a Ton of EA Data—including Valuable Source Code](#)
[Hackers begin leaking stolen data after Vice refuses to help them blackmail EA](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- **State of NY, Office of IT Services**
- **Daimler**
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymode Helps

Peace of Mind

The Top 25+ Source Code Leaks

State of New York, Office of IT Services

June 2020

A misconfigured Git repository operated by the New York State's Office of Information Technology Services exposed all projects inside it to the internet. To make matters worse, several of the projects exposed in this leak included secrets and passwords for the servers and databases in use by the associated systems. The misconfiguration allowed anyone from the internet to create a user account and login unimpeded with admin credentials.

Further Reading:

[An Internal Code Repo Used by NY State IT Office was exposed online](#)

Daimler

May 2020

A Github repository belonging to Daimler AG was discovered by a Switzerland-based software developer. The repository had been misconfigured in such a way that it allowed anyone to create an account and access the projects within it. This leak included more than 500 Git repositories and included the source code of the onboard logic units (OLUs) that connect several Mercedes vans to the cloud. The OLU allows apps to track the vans, monitor their status, or disable them if they are stolen. The safety implications that could arise from the ability to remotely track and disable vehicles is staggering.

Further Reading:

[Mercedes-Benz onboard logic unit \(OLU\) source code leaks online](#)

[Smart Car Source Code Leak May Compromise Customer Safety](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- **US Government**
- **Clearview AI**
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks

US Government

April 2020

The FBI confirmed that unidentified cyber actors accessed source code repositories of unspecified US federal agencies and private businesses through misconfigured SonarQube instances. SonarQube is an open source SAST tool used to test code for vulnerabilities and bugs. According to the CEO of SonarQube, the tool is an on-premises product, designed to sit behind the firewall within a private environment. Organizations who choose to expose it outside their firewall are supposed to configure the instances to prevent unauthenticated access. In several cases this extra configuration was not performed, allowing cyber actors to exploit the misconfiguration vulnerability to exfiltrate and publicly post proprietary code. SonarQube announced that new instances of SonarQube will have authenticated access configured by default.

Further Reading:

[Cyber Actors Target Misconfigured SonarQube Instances to Access Proprietary Source Code of US Government Agencies and Businesses](#)
[About the recent code leaks from SonarQube instances](#)

Clearview AI

April 2020

A cybersecurity firm discovered a misconfigured repository containing Clearview AI source code. The repository allowed anyone to register as a new user and access the source code needed to compile and run the Clearview AI apps. The repository also contained secret keys and credentials that allowed access to the cloud storage buckets that stored copies of Clearviews finished Windows, Mac, Android, and iOS apps, and Slack tokens that allowed password-less access to the company's internal communications.

Further Reading:

[Security Lapse Exposes Clearview AI Source Code](#)
[Breach of Clearview AI Source Code Renews Concerns About Law Enforcement Facial Recognition Programs](#)

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- **Rogers Communications**

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

[The Top 25+ Source Code Leaks](#)

Rogers Communications

January 2020

A security researcher discovered two open GitHub accounts containing application source code, internal usernames and passwords, Oracle credentials, and private crypto keys for Rogers Communications. The researcher later found five more open folders on GitHub that appeared to contain personally identifiable information of their ISP's web development team. Rogers filed a DMCA takedown request with GitHub, stating that the proprietary corporate code had been pushed into public repositories by ex-employees.

Further Reading:

[No big deal, Rogers, your internal source code and keys are only on the open web. Don't hurry to take it down](#)

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications



How to Stop Source Code Leaks

From software supply chain attacks to human error, the source code leaks highlighted above serve as a stark reminder of the need for robust defense measures across the entire software development lifecycle. To keep your most sensitive information safe, you need to build a strong security culture inside and out, secure the code itself, and respond quickly and effectively in the event of a breach.

Implement the following tips to help prevent source code leaks:

Software Supply Chain Security

When preventing source code leaks, don't overlook your third-party partners. Securing your software supply chain is essential. Evaluate their security practices, including security planning, testing, deployment, and monitoring. Implement strong contractual obligations to protect your code. Consider internal code repositories for key components instead of relying solely on external partnerships.

Secure Coding Practices

Promote and enforce secure coding practices within your development team. Encourage the use of libraries and frameworks with known security profiles and avoid common coding vulnerabilities.

Access Controls

Implement least-privilege access controls, granting access only to the tools and resources employees need for their specific tasks. Regularly review and audit access permissions to prevent unauthorized access and privilege escalation.

Multi-Factor Authentication (MFA)

Though not a silver bullet, MFA makes it much harder for hackers to gain access to sensitive systems and repositories, even if they have stolen credentials. It should be implemented on all sensitive systems, including code repositories, development environments, internal communication tools, and cloud infrastructure.

Employee Training and Incentivization

Attackers often use human engineering as a way in. Regular cybersecurity awareness training is vital. This includes teaching employees about phishing, social engineering tactics, secure password hygiene, and what to do in the case of suspicious activity. Education is just one part of the solution. To ensure

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cycode Helps

Peace of Mind

The Top 25+ Source Code Leaks



How to Stop Source Code Leaks (cont.)

cybersecurity is top of mind, employees must be consistently encouraged and motivated to follow best practices.

Continuous Monitoring and Patching

Implement real-time code monitoring to detect potential breaches and suspicious activity. Have a rapid patching process in place to address vulnerabilities quickly and minimize the window of opportunity for attackers.

Incident Response Plan

All orgs should have a well-defined incident response plan that outlines steps to take in the event of a leak. This plan should include communication protocols, containment procedures, and forensics investigation measures.

The reality is that continuous monitoring and investigation requires an incredible amount of time and resources. Fortunately, modern tools and technology can help.

Introduction

What Is a Source Code Leak?

How Is Source Code Leaked?

The Impact of a Source Code Leak

Source Code Leaks for 2020 to 2024

- Binance
- Mercedes-Benz
- Rockstar Games
- Ubisoft
- Samsung
- Twitter
- GoDaddy
- Slack
- Intel
- Uber
- LastPass
- Globant
- NVIDIA
- Nissan
- Microsoft
- Intel
- Capcom
- Embraer
- Github
- Microsoft
- Nintendo
- Electronic Arts
- State of NY, Office of IT Services
- Daimler
- US Government
- Clearview AI
- Rogers Communications

How to Stop Source Code Leaks

How Cymode Helps

Peace of Mind

The Top 25+ Source Code Leaks

How Cymode Helps Prevent Source Code Leaks

Cymode's complete ASPM platform helps prevent leaks that expose your intellectual property. Cymode ASPM delivers visibility, prioritization, and remediation to keep your source code safe.

Prevention

Cymode prevents code leaks from happening by using a number of techniques. This includes identifying anomalous or suspicious user activity and unusual repo access patterns that might indicate a unauthorized access. We also help you harden pipelines and strengthen source control systems to prevent breaches that could lead to a source code leak. Cymode automatically fingerprints proprietary repos and continuously scans public repos and code sharing sites for proprietary code. If your code is leaked, Cymode automatically alerts you so you can remove it quickly before other potentially malicious actors can access it.

Visibility

The breadth and depth of Cymode's end-to-end scanning capabilities enables security teams and developers to find API keys, tokens, proprietary information, and other secrets in source code and beyond. This includes build logs, infrastructure, kubernetes clusters, version histories, and even productivity tools like Slack and Confluence. Should your code be leaked, it is far less likely to contain sensitive information.

Furthermore, if public source code exposure is detected, Cymode can automatically create workflows to send alerts, create tickets, and resolve the exposure of private resources.

Prioritization

A code leak is bad. A code leak with secrets in it is far, far worse, though not all secrets are created equal. That's why Cymode automatically helps teams prioritize secrets remediation with customer risk scoring based on criticality, location, and likelihood of exposure. This ensures developer efforts are focused where they will be most impactful so that if your code is exposed, your secrets aren't exposed along with it.

Remediation

Cymode's developer-friendly workflows make it easier than ever to enforce secure coding best practices and stop secrets before they enter your codebase. Cymode gives developers tools they love to use in the environments they live and breathe in every day - it's not just another dashboard developers won't check.



Peace of Mind

When code is leaked, organizations suffer. Their code can be examined by malicious actors for potential defects or ways to exploit it or by competitors interested in learning trade secrets. Exposed secrets often give attackers an easy way into high value targets, where they can sit undetected for months, doing significant damage. The organization suffers loss of trust and damage to their brand reputation. They may also be slapped with a hefty fine should PII or other sensitive data be exposed. No one wants to be the latest headline.

The good news is that Cyscale's multifaceted approach to pipeline security, secrets security, and leak prevention can help you stop a leak before it occurs. That kind of peace of mind is priceless.

Want peace of mind that your source code is safe?
[Book a demo now](#)

