Software Supply Chain + Version Control Systems Vulnerabilities Timeline

DARKOWL

DarkOwl has 9.3 Million documents containing links to software shared on **Github.**

APR 2022

LAPSUS$ shared screenshots as proof of their privileged access to **Okta** on **Telegram.**

MAR 2022

Gitlab identifies critical vulnerability that allows remote attackers to take over accounts.

Cycode identified three major risks in **Github Actions** in the workflow queuing model and runner environment.

FEB 2022

Gitlab identifies several critical enterprise edition vulnerabilities where unprivileged users can add other users to groups through an API endpoint and environment variables can be leaked via the sendmail delivery method.

LAPSUS$ successfully infiltrated **Okta,** and subsequently accessed sensitive data for at least 360 additional victims via Okta's client interface.

JAN 2022

NOV 2021

Gitpaste-12, the first ever worming botnet, is discovered.

UA-Parser-JS NPM library infected and altered to steal passwords along with critical browser identification parameters.

OCT 2021

Researchers from **Cidr Security** surfaced a security flaw within **Github Actions** and system permissions of **GITHUB_TOKEN.**

AUG 2021

Critical vulnerabilities discovered in the **Python Package Index** that could arbitrarily execute code and take full control of the official software repository.

REvil ransomware attack via **Kaseya.**

JUL 2021

DarkOwl observes Russian malware developers on the AntiChat Telegram channel recommending developers run **Github Actions** locally to test malicious code injections before the official push and/or pull to the target repository.

MAY 2021

Data broker, **ShinyHunters,** compromises **Microsoft's Private Github account.**

Codecov alerts customers that their **Bash uploader** had been compromised.

APR 2021

MAR 2021

Unknown threat actor compromises the **PHP Git repository,** creating a backdoor for malicious remote code execution. Github discovers it is the source of a major supply chain attack against the Java integrated development environment (IDE).

Attackers use **Bitbucket** to spread malware and compromise 500,000 victims.

FEB 2021

Github detects a widespread cryptocurrency mining campaign that infected thousands of repos across their servers.

DEC 2020

Solarwinds supply chain attack.

Blueleaks files – law enforcement identifies malicious Python packages in circulation.

JUN 2020

OCT 2018

Microsoft acquires **Github** for $7.5 billion USD.

Gitlab founded.

OCT 2011

APR 2008

Github launched.

Git architecture first developed.

APR 2005

Interested in learning more about how DarkOwl can help with your use case?

Contact Us

NEW RESEARCH

Version Control Systems and Software Supply Chain Risk

Read Report