可以说，这是有史以来最大范围的一次源代码泄露。

> 源代码就是指编写的最原始程序的代码，主要对象是面向开发者，我们平常使用的应用程序都是经过源码编译打包以后发布呈现的。
>
> 公司专有程序代码对于网络创意公司来说是其生命的化身，掌握了其编写方式，就可以复制出一个相同的程序，或通过阅读源代码找到程序的漏洞进行任意攻击。所以在互联网兴起后世界各国都立法对其进行保护。

微软、Adobe、联想、AMD、高通、联发科、通用电气、任天堂、迪士尼、华为海思等 50 家科技公司都中招了。

据外媒报道，遭泄露的源码被发布在 GitLab 上一个公开存储库中，并被标记为“exconfidential”（绝密），以及“Confidential & Proprietary”（保密&专有）。

> 雷锋网注：GitLab 是一个用于仓库管理系统的开源项目，全球第二大开源代码托管平台，谷歌重金投资加持的开源独角兽，阿里巴巴还一度是其重要客户。

根据安全研究人员 Bank Security 提供的信息，该存储库中大约包含了超过 50 家公司的源码。但有一些文件夹是空的，还有一些存在硬编码凭证。（一种创建后门的方式。）

此外，开发人员 Tillie Kottmann 提到，一些代码库中确实存在硬编码凭证，他在发布前已尽可能地将其删除，“以避免造成直接伤害或是助长更大的破坏”。另外，他也坦承自己并未在发布前与每一家受影响的公司进行联系，但他们确保自己“尽了最大的努力将负面影响最小化”。

Kottmann 的 Twitter 账户简介写道，“这里可能正在泄露您的源代码。”该账户的置顶推文是一条众包帖，问道“您认为机密信息、文档、二进制文件和源代码，哪一种最应该向公众公开……”

使用错误的 Devops 工具暴露了代码

对于上述事件，不少安全专家表示，“在互联网上失去对源代码的控制，就像把银

行的设计图交给抢劫犯一样。”

目前，Kottmann 已应部分企业的要求删除了代码。例如 Daimler AG，梅赛德斯-奔驰的母公司；联想的文件夹也已经空空如也。针对有移除代码要求的公司，Kottmann 表示愿意遵守，并乐意提供信息，“帮助公司增强基础架构的安全性”。

而关于源代码泄露的原因，开发团队也在继续寻找原因。

Kottmann 称，他们试图在发布硬编码凭证之前从公司的源代码中删除这些硬编码凭证，这些凭证通常用于创建后门程序，以免发生更加强大的安全漏洞。

回顾在 Kottmann 的 GitLab 服务器上泄漏的一些代码，可以发现某些项目已由其原始开发人员公开发布，或者在很久以前进行了最后更新。

不过，开发人员表示，有更多公司使用错误的 Devops 工具配置了暴露源代码的公司。此外，他们正在探索运行 SonarQube 的服务器，SonarQube 是一个开源平台，用于自动代码审核和静态分析，以发现错误和安全漏洞。

Kottmann 认为，有成千上万的公司由于未能正确保护 SonarQube 安装而暴露了专有代码。

不过，网络安全公司 ImmuniWeb 的创始人兼首席执行官 Ilia Kolochenko 指出，“从技术角度来看，这次的泄露并不算很严重……若没有每天的支持和改进，源代码也会迅速贬值”。

尽管如此，这样大规模的泄露事件原因还是值得引起注意。

代码被公开之痛

每一次源代码被公开，伴随着的都是巨大的损失。

我们举几个例子，大家就明白了。

大家一定还记得大疆前员工将含有公司商业机密的代码上传到了 GitHub 的公有仓库中，造成源代码泄露的事件。

根据当时的报道，这些源代码，攻击者可以 SSL 证书私钥，访问客户的敏感信息，比如用户信息、飞行日志等等。

根据评估，这次泄漏代码一共给大疆造成了 116.4 万的经济损失。

再比如，2019 年 4 月，B 站整个网站后台工程源码泄露，并且“不少用户密码被硬编码在代码里面，谁都可以用。”

当天，在开源及私有软件项目托管平台 GitHub 上，出现了名为“哔哩哔哩bilibili网站后台工程源码”的项目。据悉，该项目由账号“ openbilibili ”创建，由于网站的开源性质，登录网站者均可使用。当日 B站股价跌 3.27%。

虽然很快被封禁，B 站也已经报警处理，但有不少网友克隆了代码库，隐患已经埋下，补救起来也颇为头疼。

当然，除了主动泄露私钥，还有很多人在 GitHub 上把登录信息和明文密码也都一起开源的。

而这些被开源的代码一旦被黑客利用，造成的损失就要看黑客的心情了。

附源代码泄漏完整受害者列表：

Johnson Controls（江森自控）

iLendx （联想）

Banca Nazionale del Lavoro

Lenovo-smart-display-7

Adobe

Fastspring

GE Appliances（GE电器）

Mercury TFS

GovCloudRecords

MyDesktop

eMasurematics

Buckzy

TeamApt

Alpha FX

Covid Apps

Romeo Power

Digital Health Department

DRO Health

Elgin Industries

Berkeley Lights

Pwnee Studios

NYNJA

Tapway

BlocPower

Capital Technology Services

Lenovo（联想）

AMI

insyde

Erobbing / Luobin They make various Android based devices, like DVRs and Law Enforcement devices. http://www.erobbing.com/

KaiOS

AMD

Chenyee / Gionee

Disney（迪士尼）

Mineplex

Daimler

Rockchip

HiSilicon（海思）

Aukey

Chunmi

Xiaomi's Kitchen Appliance Subsidiary

PUKKA

Roblox Corporation

Microsoft（微软）

Motorola（摩托罗拉）

Qualcomm（高通）

Mediatek（联发科）

Bahwan CyberTek

CryptoSoul

gms

ReactMobile

ЦЭККМП

Tactical Electronics

Siasun

雷锋网雷锋网雷锋网

参考资料：

【1】https://www.bleepingcomputer.com/news/security/source-code-from-dozens-of-companies-leaked-online/?

【2】https://gitlab.com/gitlab-com/www-gitlab-com/issues/5555