ENISA《欧盟协调漏洞披露政策》概述

监管 (https://www.secrss.com/articles?tag=监管) · 信息安全与通信保密杂志社 (https://www.secrss.com/articles?author=信息安全与通信保密杂志社) · 2022-04-15

报告全面概述欧盟成员国和美国、日本、中国在协调漏洞披露的现状和主要措施，概述欧盟在实施CVD政策时面临的各种挑战并提出了具体建议。

2022年4月13日，欧洲网络及信息安全局发布《欧盟协调漏洞披露政策》（Coordinated Vulnerability Disclosure Policies in the EU）报告，报告称，目前漏洞披露已成为致力于加强欧盟网络安全弹性的网络安全专家关注的焦点，报告全面概述欧盟成员国和美国、日本、中国在协调漏洞披露的现状和主要措施，概述欧盟在实施CVD政策时面临的各种挑战并提出了具体建议。

报告主要包含4个章节内容。

第一章节

欧盟协调漏洞披露政策现状

目前欧盟各成员国在制定以及执行CVD政策方面的进展不尽相同，目前的情况是比利时、荷兰、法国等4个国家已经制定了国家层面的CVD政策，捷克、意大利、西班牙等10个国家还在政策制定过程中，丹麦、德国等4个国家正在制定的初始阶段，而波兰、瑞典等9个国家则尚无这方面的打算。从CVD制定进展情况来看，西欧国家相对于其他欧洲区域更加成熟，南欧国家以及中欧和东欧国家在这一进程中却落在后面。其中，荷兰、比利时、立陶宛是欧盟各成员国中建立了最有效CVD国家，荷兰最重要的成功因素是采用自下而上的方法来建立目前的CVD。这一过程始于该国的主要银

行和互联网服务提供商，他们感到迫切需要在寻找漏洞时接纳合乎道德准则的黑客。立陶宛国家网络安全中心制定的CVD可作为起草欧盟一级最佳做法的基础的程序。比利时则是为研究人员提供全方面的保护。

国家	现状	CVD政策制定情况
比利时	比利时制定有CVD政策，该政策可以能够为研究人员提供全面保护。	已经制定
保加利亚	保加利亚尚未制定CVD政策，但国家CERT参与了CVD政策的制定。	未制定
捷克	捷克希亚没有制定CVD政策。国家CERT正在评估减少漏洞的各种方案，其中包括正在制定的一项国家CVD政策。	正在进行中
丹麦	丹麦正处于制定CVD政策的初始阶段。	初期
德国	德国没有制定CVD的国家政策。德国联邦议会正在制定CVD政策，它将应被视为德国的国家政策。	初期
爱沙尼亚	爱沙尼亚尚未实施CVD政策。漏洞是通过国家制定的一系列法规来处理。	未制定
爱尔兰	爱尔兰没有制定政策，执行政策也不被视为优先事项。	未制定
希腊	希腊尚未实施CVD政策，但在制定CVD政策上采取了积极立场。	正在进行中
西班牙	西班牙没有全国性的CVD政策，目前正在建立国家级的CVD框架	正在进行中

法国	法国已经制定CVD政策。	已经制定
克罗地亚	克罗地亚尚未制定CVD政策，目前也没有制定这项政策的计划。	未制定
意大利	意大利没有制定CVD政策。关于CVD政策的讨论正在进行中。	正在进行中
塞浦路斯	塞浦路斯没有制定CVD政策。	未制定
拉脱维亚	拉脱维亚没有CVD政策，但年底将制定一项正式的CVD政策。	初期
立陶宛	立陶宛制定了CVD政策，并在“立陶宛共和国网络安全法修正案”中予以正式规定。	已经制定
卢森堡	卢森堡没有正式的CVD政策。国家CERT发布了一项CVD政策，目前正在就CVD政策进行讨论。	正在进行中
匈牙利	匈牙利尚未制定CVD政策。目前正在就“匈牙利网络安全法”修正案进行讨论，特别是纳入脆弱性披露要求。	正在进行中
马耳他	马耳他尚未制定CVD政策，目前也没有制定这一政策的计划。	未制定
荷兰	荷兰制定有CVD政策，能够为研究人员提供全面保护。	已经制定
奥地利	奥地利目前尚未制定CVD政策	正在进行中
波兰	波兰未制定CVD政策	未制定
葡萄牙	葡萄牙没有制定CVD政策，但已经成立了一个工作队来负责相关工作	初期
罗马尼亚	罗马尼亚尚未实施CVD政策，在这方面没有取得任何进展。	未制定
斯洛文尼亚	斯洛文尼亚尚未实施CVD政策。该国计划在下一个网络安全战略中纳入CVD政策。	正在进行中
斯洛伐克	没有制定CVD政策，而在立法层面正在建立相应的程序。	正在进行中
芬兰	芬兰没有制定反补贴政策，但已开始朝着这一方向努力。此外，国家CERT还发布了CVD政策。	正在进行中

瑞典	在国家一级没有制定CVD政策，也没有在现阶段制定这种政策的计划。	未制定

第二章节

美国、日本、中国的CVD现状

美国的协调漏洞披露由网络安全与基础设施安全局（CISA）负责，主要包括接收、分析、缓解协调、缓解措施的适用以及公开等五个步骤。

· 接收 在收到报告时，CISA进行初步甄别，以确保漏洞的准确性， CISA进行漏洞分析，检查有关软件漏洞的公共信息。

· 分析 CISA与供应商合作，通过检查技术问题和它可能带来的风险来研究该漏洞。

· 缓解协调 继续与供应商密切合作，CISA将通过开发缓解(例如补丁或更新)来找到解决问题的方法。

· 缓解措施的适用。受影响的最终用户必须在公开披露之前测试和应用缓解措施。这种情况发生在这个阶段。

· 公开 CISA将通过其通道将该漏洞通知受影响的用户。必须强调指出，这一阶段的特点是中钢协、受影响的供应商和脆弱性报告的来源之间进行了协调。

随着网络威胁的不断增加和演变， CISA可以帮助确定和实施这一进程中的最佳实践。

在日本，软件等产品中漏洞的协调披露是根据“信息安全预警伙伴关系准则”进行的。研究人员的漏洞报告被发送给信息技术促进机构，负责初步分析和分类工作。接着，报告被发送给JPCERT协调中心，负责与产品的供应商/开发人员进行协调。一旦供应商/开发人员解决了该漏洞，将在日本漏洞说明(JVN)上发布咨询意见，通常与供应商/开发人员的咨询一起发布。通过这一协调一致的漏洞披露过程，截至2021年3月，在JVN上总共发布了1 875份咨询意见。自从本指南发布以来，许多供应商/开发人员已经接受了协调的漏洞披露过程。

中国的漏洞评估过程是以信息部门为主导的。在国家漏洞数据库公布之前，将对高度威胁的漏洞在信息行动中的效用进行评估，并根据这些高威胁漏洞的影响来决定发布时间。报告称，中国政府正考虑出台具体规则，规定如何披露漏洞，并要求研究人员在公布漏洞之前向有关部门报告。

第三章节

欧盟协调漏洞披露政策的挑战

欧盟协调漏洞需要应对来自法律、经济等方面的挑战。因此，各国在制定CVD时，需要评估以下方面的挑战在多大程度上阻止了CVD的制定和实施。

· 法律障碍。安全研究人员面临着重大的法律风险。

· 利益攸关方之间缺乏合作。

· 政府对漏洞利用的模棱两可。

· 市场激励有限。鼓励安全研究人员参与协调的脆弱性披露方案。

· 财政和人力资源挑战。缺乏资源和技能，缺乏执行和运作费用。

第四章节

建议措施

对欧盟各成员国的分析得出的主要建议包括：

修订刑法和网络犯罪指令，为参与漏洞发现的安全研究人员提供法律保护；

在为安全研究人员建立任何法律保护之前，定义明确区分“道德黑客”和“黑帽”活动的具体标准；

通过国家或欧洲漏洞赏金计划，或通过促进和开展网络安全培训，为安全研究人员制定积极参与 CVD 研究的激励措施。

除上述内容外，还针对经济和政治挑战提出了其他建议：

关于法律挑战的建议：国家刑法应该对安全研究人员提供免责的可能性，会员国可以修订其刑法，为参与发现脆弱性的研究人员创造法律确定性和必要的“安全港”，同时也承认道德黑客行为。修订“网络犯罪指令”，以便为参与发现脆弱性的安全研究人员提供法律确定性，并允许界定各成员国的共同规则和程序，以便在欧洲建立一个协调的漏洞披露共同程序。

关于经济挑战的建议：成员国需要促进旨在鼓励安全研究人员积极参与CVD制定，并在欧盟一级建立支持，比如成立欧洲委员会自由和开放源码软件审计项目予以推动。欧盟必须提供适当的资金支持和方案，使欧盟的CVD政策可行，建立一个非营利和资源充足的国际实体促进跨境协调的实现。

报告最后指出，欧盟应该就如何制定CVD政策、公布各国的最佳做法和挑战以及公布各国可据以起草其政策的模板，向各国提供明确的指导并发布最佳实践。此外，ENISA 将需要开发和维护一个欧盟漏洞数据库这项工作将补充现有的国际漏洞数据库。

原文下载链接：

https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

监管 (https://www.secrss.com/articles?tag=监管)

相关资讯

南昌市某企业IP疑被黑客远控并滥用，当地网信办罚款5万元
(https://www.secrss.com/articles/70934)

监管 (https://www.secrss.com/articles?tag=监管) · 网信南昌 (https://www.secrss.com/articles?author=网信南昌) · 2024-09-30

明文存储用户密码，美国互联网巨头Meta违反GDPR被罚超7亿元

(https://www.secrss.com/articles/70777)

互联网 (https://www.secrss.com/articles?tag=互联网) · 安全内参 (https://www.secrss.com/articles?author=安全内参) · 2024-09-29

谨慎使用风险突出的5类弱口令类型 (https://www.secrss.com/articles/70469)

监管 (https://www.secrss.com/articles?tag=监管) · 国家网络安全通报中心 (https://www.secrss.com/articles?author=国家网络安全通报中心) · 2024-09-21