区块链智能合约漏洞 修复困难

■ 高 枫

最近区块链平台 EOS 智能合约漏洞事件再次把区块链安全推上了风口浪尖。攻击者可以通过发布包含恶意代码的“智能合约”，经过一系列的操作之后，控制区块链网络中的所有节点，从而为所欲为。从 The DAO 到 BEC，SocialChain，Hexagon，再到这几天的 EOS 漏洞，“智能合约”已经成为区块链安全的重灾区。

那么什么是智能合约，智能合约的漏洞究竟给安全带来了什么样的新挑战，我们应该如何应对？本文中 360 代码卫士团队的安全专家将结合自身在区块链智能合约漏洞方面的研究成果和心得体会，从这几个方面进行深入解读。

一、什么是智能合约

智能合约 (smart contract) 这个术语是在 1994 年由 Nick Szabo 提出的，后来经过几次在不同环境下的重新定义。我们现在通常所说的区块链智能合约以以太坊为代表，以太坊的作者 Vitalik Buterin 意识到，在区块链系统中，交易逻辑是可以和底层系统机制分离的。

底层系统负责交易块的创建和验证，记账者的共识达成等基础功能，而交易本身到底做什么事情是可以通过二次编程的方式来定义的。因此他设计了一种交易代码执行的虚拟环境 EVM，使用者可以开发自定义的交易逻辑，发布到链上，当交易进行时，链上所有的节点都执行相同的代码，从而同步改变链上数据的状态。他为这种代码使用了“智能合约”这个名字，这是我们目前通常所说的智能合约的内涵。

二、智能合约漏洞，左右为难

智能合约本质是一段运行在区块链网络中的代码，它完成用户所赋予的业务逻辑。以以太坊体系的代币为例，其业务逻辑是代币发币和交易。以太坊在设计之初，将智能合约设计成了一旦部署就不能修改的模式。这种设计有可能是为了提高智能合约的可信性。

但是我们知道，只要是由人编写的程序，就一定会出现错误和缺陷。以太坊这种设计本身就违背了程序设计的一般规律，在智能合约出现漏洞的时候可能会造成无法弥补的损失。我们可以看到，近期出现的以太坊体系智能合约的漏洞，造成了巨大的影响，有的代币也因此毁灭。

目前以太坊体系区块链智能合约的机制设计，加之漏洞可能带来的毁灭性影响，使得已上线智能合约的漏洞的报告和处理变得非常棘手。

360 代码卫士团队在近期的研究中发现了以太坊体系下多个已上市交易的代币的智能合约安全漏洞，并已第一时间报告厂商，但到目前为止厂商尚未作出任何回应。对于厂商来说，由于智能合约不可修改的特性，要对上线后发现的漏洞进行有效修复，只能选择重新部署新的合约，这将付出巨大的代价，因此有的厂商可能会选择不响应不处理。

而对于安全研究者来说，也面临左右为难的尴尬境地。在厂商修补漏洞前公开漏洞细节对于厂商不利，有悖漏洞披露的一般原则，但如果厂商迟迟不修补漏洞，公众对于漏洞的存在不知情，风险会随着时间的增长迅速膨胀，漏洞一旦爆发可能会造成更大的危害，波及更大的人群，可能会造成很多人的投资瞬间化为乌有。

三、智能合约漏洞，如何应对

在一些联盟链中，智能合约的设计是可以在部署之后更新的，当然这种更新需要一定的线下协商流程。要应对区块链智能合约的安全漏洞问题，未来需要普遍考虑设计相应的智能合约协商更新机制，降低漏洞修复的成本。

但现在，我们需要面对现实，做出几乎唯一可行的、切实有效地努力——在智能合约上线之前，对其进行全面深入的代码安全审计，尽可能的消除漏洞，降低安全风险。

360 代码卫士团队安全专家表示，当前区块链智能合约中可能出现的漏洞至少有 20 余种。以下列举一些常见的区块链智能合约的漏洞类型及其可能造成的风险，这些漏洞在智能合约上线之前，都应该进行详细的排查。

1. 整数溢出

智能合约中危险的数值操作；

可能导致合约失效、无限发币等风险。

2. 越权访问

智能合约中对访问控制处理不当；

可能导致越权发币风险。

3. 信息泄露

硬编码地址等；

可能导致重要信息的泄露。

4. 逻辑错误

企业邮箱被黑客攻击了怎么办

■ 宋明成

企业邮箱的安全问题一直是各大企业关注的问题，而当我们在日常工作中又该如何做好安全防护？遇到问题时又该如何处理解决？

如何判断是否遭到黑客攻击

我收到客户发来的汇款信息，通过电话核对，发现信息并非客户所发，此时如何判断是我的邮箱被黑客攻击了还是客户的邮箱被攻击了？

针对这种情况，一般的解决方法是：

1 用户自身检查有没有被设置过自动转发 、来信分类中的转发功能和代收功能；

2 在“自助查询”中查看是否有异常登录过的 IP 或地域。

建议用户在需要传输重要信息时对信息使用加密的功能，以防止信息在传输的过程中被窃听。

SSL 技术在邮件系统中的应用比较广泛，尤其是在企业和电子政务等需要较高保密性的场合。使用 SSL 技术不但能够有效的对用户的密码进行加密，而且能够对邮件的内容本身进行加密，防止邮件在网络传输的过程中被窃听。

目前在 Coremail 电子邮件系统中，SSL 技术结合主要应用在 POP3、SMTP、IMAP 和 HTTPS 服务上。通过使用 SSL 技术极大地增强了邮件系统的安全性，而整个加密解密的过程对用户来说几乎是透明，用户只需访问特定的端口或者在邮件客户端进行简单的设置即可。Coremail SSL 已经成功应用到各大运营商，大型企业商务交流，政府政务和市民信箱中，是客户邮箱信息安全的重要保障。

电子邮件怎么传播病毒

电子邮件传播病毒都是通过附件的吗？点开陌生人发来的邮件，只有文字没有图片、连接以及附件，会感染病毒吗？

是的，病毒一般通过附件传播。陌生人发来的邮件，只有文字，一般不会中病毒。但是尽量不要去点开已经被判断为病毒邮件的邮件。

常见的病毒邮件案例都是通过图片和脚本文件(.js、.reg、.bat、.exe)进行传播，而传染的平台多数为 Windows。如果接触到有这样邮件不建议打开。

如何避免成为垃圾邮件

我在外贸公司工作，需要经常给国外的客户发邮件，为什么我的邮件会被对方邮箱默认为垃圾邮件？

被判断为垃圾邮件的原因常见如下：

1、IP 信誉度低

出现信誉度低的情况可能是有站内用户在发送垃圾邮件，导致 IP 被 反垃圾联盟组织加入了 RBL 中。邮件管理员需要定期将这些用户找出并限制。

用户如果网络环境出口 IP 是与其他业务系统共用的情况下，会容易被反垃圾联盟组织列入 RBL 中。建议是只给邮件系统单独一个出口 IP。

通过增加 SPF 和 PTR 记录可以有效提供 IP 的信誉度，SPF 需要联系域名供应商进行添加，PTR 记录需要联系网络供应商添加。

2、对方邮件服务器规则设定

Gmail，Hotmail 出现该情况需要通过其他方式联系收件方，可对发件人域名或地址增添白名单策略进行放宽规则。

除以上管理员需要操作之外，Coremail 论客“海外转发”功能在国外架设了多台海外中转服务器，并不断优化国际访问路径，从根本上解决了海外邮件不畅通的问题。

建议在设置邮箱密码时不要选择过于简单的密码组合，合理密码设置将加大邮箱被黑客攻击的成功率。而身份证后 6 位及出生日期也是黑客最容易破解的密码形式。

科普小知识：企业邮箱的安全重要性：企业邮箱是企业对内外交流与商务活动的重要途径，在商务活动及日常工作中，通过邮件能更快捷方便地将信息进行传递解决。企业在邮件使用中通常会附上公司或客户的信息，一旦这些信息被盗取、泄露，将导致企业在公众的威信和信任度下降，严重者将直接造成经济财产损失。

代理转账函数缺失必要校验；

可能导致基于重入漏洞的恶意转账等风险。

5. 拒绝服务

循环语句、递归函数、外部合约调用等处理不当；

可能导致无限循环、递归栈耗尽等拒绝服务风险。

6. 函数误用

伪随机函数调用和接口函数实现问题；

可能导致可预测随机数、接口函数返回异常等风险。

漏洞永远都会存在。未来区块链行业一定会出现更多的安全问题，之前传统互联网领域里面遇到的安全问题，区块链行业里面一定也会遇到。区块链行业要能够与网络安全行业做到协同开放，才能使行业更加健康稳定安全地发展。