奇安信
新一代网络安全

PhpStudy 后门事件

安全预警通告

奇安信安全监测与响应中心

2019 年 09 月 23 日

目录

第1章 安全通告

尊敬的客户：

近日，使用广泛的 PHP 环境集成程序包 PhpStudy 遭遇供应链攻击，其自带的 php_xmlrpc.dll 模块存在后门，并且此后门藏匿于软件的功能性代码中，极难被发现。目前也尚无杀毒软件可对此后门进行扫描查杀。该后门影响数十万的 PhpStudy 软件安装实例，后门植入者或知晓此后门的人员（目前此后门事件已在行业内传播扩散）可利用此后门执行蠕虫式的传播攻击。

强烈建议使用该 PHP 环境集成程序包的用户立即自查自杀，并更新到最新版本。

奇安信安全监测与响应中心将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 文档信息

文档名称	PhpStudy 后门事件安全预警通告
关键字	PhpStudy，后门，蠕虫
发布日期	2019 年 09 月 23 日
分析团队	奇安信安全监测与响应中心

第3章 漏洞信息

3.1 漏洞描述

近日，使用广泛的 PHP 环境集成程序包 PhpStudy 遭遇供应链攻击，其自带的 php_xmlrpc.dll 模块存在后门，并且此后门藏匿于软件的功能性代码中，极难被发现。目前也尚无杀毒软件可对此后门进行扫描查杀。在国内有着近百万 PHP 语言学习者、开发者用户使用 PhpStudy，所以此后门可能影响数十万的 PhpStudy 软件安装实例。

奇安信威胁情报中心红雨滴团队对相关的技术细节进行了深入分析后发现：

1. 植入的后门代码会连接远端的 C&C 服务器并执行相关命令。
2. 当 C&C 服务器失效时，攻击者可在无需用户验证的情况下，向受影响的服务器提交代码并执行。
3. 由于可能存在后门的软件部署量巨大，可被攻击者或知晓此后门的人员（目前此后门事件已在行业内传播扩散）利用，从而执行蠕虫式的传播攻击。

奇安信安全监测与响应中心强烈建议使用该 PHP 环境集成程序包的用户立即自查自杀，并更新到最新版本。

3.2 风险等级

奇安信安全监测与响应中心风险评级为：高危

预警等级：蓝色预警（一般事件）

第4章 影响范围

暂无完整明确的受影响版本列表

第5章 处置建议

请使用奇安信 PhpStudy 专杀工具检查是否存在后门，如果存在后门，删除老版本并从以下官网链接下载最新版本安装：

https://www.xp.cn/

- **奇安信专杀工具**

此专杀工具用于扫描 PhpStudy 环境是否被植入后门。

- **专杀工具使用方法**

请见随此预警发送的使用文档。

第6章 产品解决方案

奇安信网神天堤防火墙产品防护方案

奇安信新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，已通过更新 IPS 特征库完成了对该漏洞的防护。建议用户尽快将 IPS 特征库升级至最新的特征库**“ 1909222245” 及以上版本并启用规则 ID: 5386 进行检测。**

奇安信网神网络数据传感器系统产品检测方案

奇安信网神网络数据传感器（NDS3000/5000/9000 系列）产品，已具备该漏洞的检测能力。规则 ID 为：**5386**，建议用户尽快升级检测规则库至 **1909222245** 及以上版本并启用该检测规则。

奇安信天眼产品解决方案

奇安信天眼新一代威胁感知系统在第一时间加入了该漏洞的检测规则，请将规则包升级到 3.0.0922.11343 及以上版本。规则名称：PhpStudy 远程命令执行攻击，规则 ID：0x1002070B。奇安信天眼流量探针（传感器）升级方法：系统配置->设备升级->规则升级，选择“网络升级”或“本地升级”。

360 网神虚拟化安全管理平台已更新入侵防御规则库

360 网神虚拟化安全管理平台无代理版本可通过更新入侵防御规则库到 10172 版本，支持对 PhpStudy 远程代码执行漏洞的防护,，请用户联系技术支持人员获取规则升级包对虚拟化产品无代理版本进行升级。

360 网神虚拟化安全管理平台轻代理版本可通过更新入侵防御规则库到 2019-09-23 版本，支持对 PhpStudy 远程代码执行漏洞的防护,，请用户联系技术支持人员获取规则升级包对虚拟化产品轻代理版本进行升级。

第7章 参考资料

[1] https://www.xp.cn/