Drupal 远程代码执行漏洞（CVE-2018-7600）通告

文档信息

编号	360TI-SV-2018-009
关键字	CVE-2018-7600 Drupal
发布日期	2018 年 4 月 13 日
更新日期	2018 年 4 月 13 日
TLP	WHITE
分析团队	360 威胁情报中心

通告背景

Drupal CMS 是一款开源的用 PHP 实现的内容管理系统，在业界被广泛使用。Drupal 目前支持超过 100 万个站点，而且在前 1 万个最流行站点中的占据约为 9%市场份额。

2018 年 3 月 28 日，Drupal 官方发布新补丁和安全公告，称 Drupal 6、7、8 多个子版本存在远程代码执行漏洞(CVE-2018-7600)。目前漏洞相关的技术细节已经公开， 2018 年 4 月 13 日凌晨有相应的漏洞利用验证程序在互联网上公开，360 威胁情报中心证实攻击方法可用，所以此漏洞已经构成较大的现实威胁。360 威胁情报中心特此通告提醒用户和企业尽快采取必要防御应对措施以保障网站的安全性和可用性。

漏洞概要

漏洞名称	Drupal 远程代码执行漏洞				
威胁类型	远程代码执行	**威胁等级**	高	**漏洞 ID**	CVE-2018-7600
漏洞利用条件					
可远程访问 Drupal 站点即可。					
漏洞利用场景					
攻击者无需在目标站点上注册或认证，仅需访问存在漏洞站点的某个 URL 就可能控制网站。					
受影响版本					
确认受影响的型号： Drupal 6.x、7.x、8.x					
不受影响影响系版本					
Drupal 7.58、8.3.9、8.4.6、8.5.1					

漏洞描述

Drupal 是一种使用面非常广泛的 PHP 语言实现的内容管理系统。

Drupal 团队将这个漏洞命名为“Drupalgeddon2”，漏洞编号是 CVE-2018-7600。攻击者无需在目标站点上注册或认证，所需要做的就是访问一个 URL。而且漏洞相关 PoC 已经于 2018 年 4 月 13 日凌晨在互联网公开并证实可用。

影响面评估

360 威胁情报中心已经确认公开的 PoC 利用代码有效，且该漏洞整体影响面较大（国内受影响站点数量相对较少，大多数受影响站点位于国外），综合分析威胁等级为高。此漏洞极有可能被用于大规模地获取对站点的控制，构建 Botnet 用于可能的挖矿、拒绝服务、勒索等恶意活动。

修复方法

升级版本：

推荐更新到 Drupal 相应的最新子版本

7.x 版本，更新到 7.58
https://www.drupal.org/project/drupal/releases/7.58

8.5.x 版本，更新到 8.5.1
https://www.drupal.org/project/drupal/releases/8.5.1

8.4.x 版本，更新到 8.4.6
https://www.drupal.org/project/drupal/releases/8.4.6

8.3.x 版本，更新到 8.3.9
https://www.drupal.org/project/drupal/releases/8.3.9

使用 Patch 处置措施：

如果不能立即更新，请使用对应版本的 Patch 文件进行修补。
8.5.x、8.4.x、8.3.x Patch 地址:
https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f

7.x Patch 地址:
https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=2266d2a83db50e2f97682d9a0f

b8a18e2722cba5

参考资料

https://www.drupal.org/sa-core-2018-002
https://groups.drupal.org/security/faq-2018-002
https://research.checkpoint.com/uncovering-drupalgeddon-2/

更新历史

时间	更新
2018 年 3 月 28 日	初始报告
2018 年 3 月 28 日	补充内容
2018 年 4 月 13 日	增加确认 PoC 可用的内容，并公开发布安全通告