安全漏洞通告

CVE-2020-36193：Drupal 目录遍历漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-01-22

报告信息

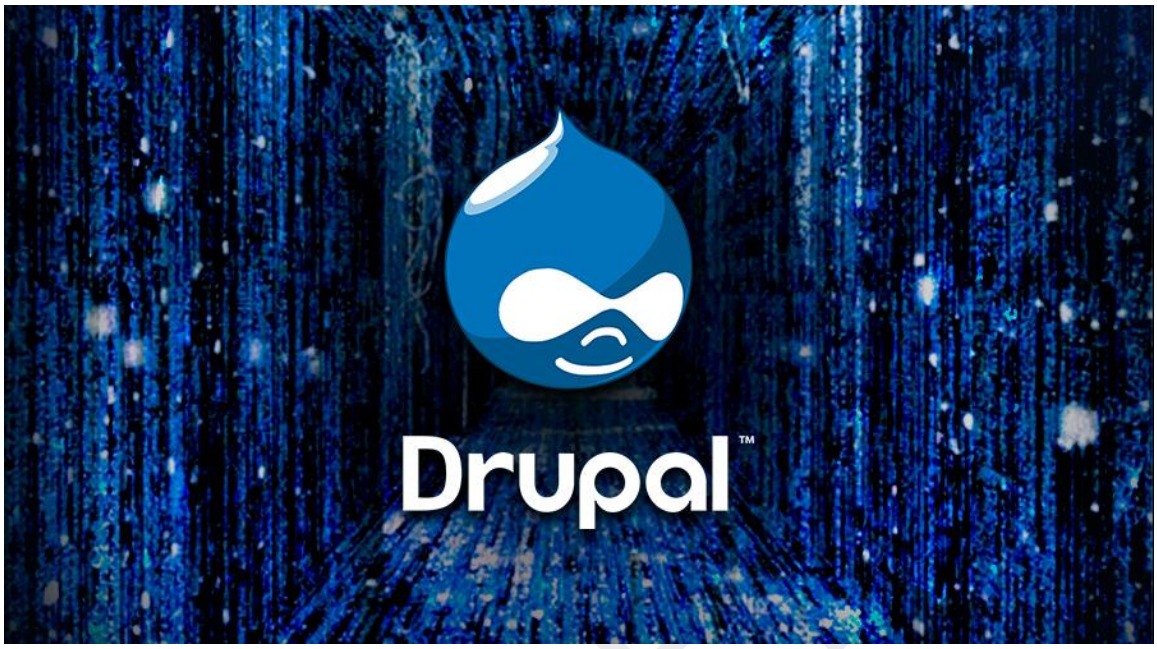
报告名称	CVE-2020-36193：Drupal 目录遍历漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-012201
报告版本	1	**报告日期**	2021-01-22
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-01-22	360CERT	360CERT	撰写报告

目录

一、 漏洞档案



漏洞类型	文件上传漏洞
CVE 编号	CVE-2020-36193
相关厂商	Drupal
相关组件	暂无
威胁等级	高危
影响面	广泛
360CERT 评分	7.2
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-01-22
报告生成时间	2021-01-22

二、 漏洞简述

2021 年 01 月 22 日，360CERT 监测发现 Drupal 发布了 Drupal 文件上传漏洞的风险通告，该漏洞编号为 CVE-2020-36193 ，漏洞等级：高危，漏洞评分：7.2。

远程攻击者通过上传特殊构造的.tar、.tar.gz、.bz2、.tlz 文件 ,可造成 任意代码执行。

对此，360CERT 建议广大用户及时将 Drupal 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
360CERT 评分	7.2

四、 漏洞详情

CVE-2020-36193: 文件上传漏洞

Drupal 是使用 PHP 语言编写的开源内容管理框架（ CMF ），它由内容管理系统（ CMS ）和 PHP 开发框架（ Framework ）共同构成。

pear，composer 是 php 的插件管理/包管理系统，目前 composer 更为通用和流行。

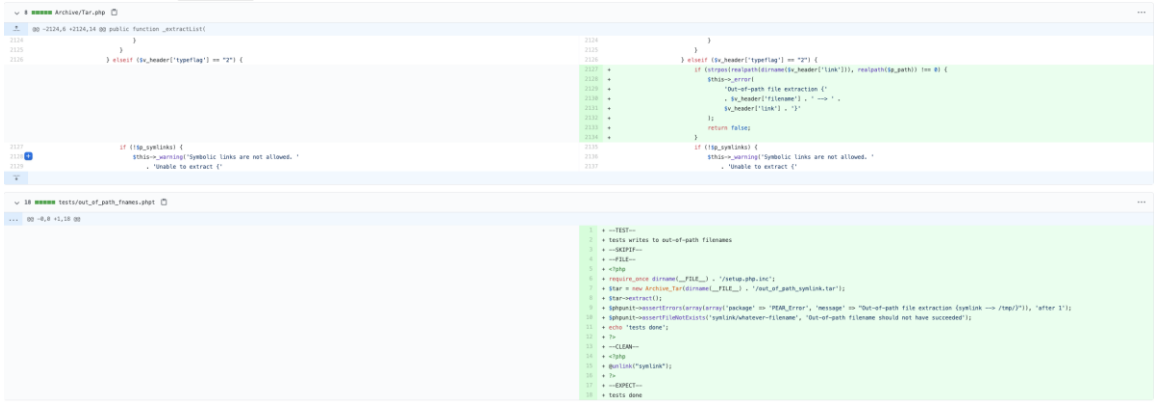
drupal 使用 composer 作为包管理系统，并引用了存在严重漏洞的 "pear/archive_tar": "1.4.11"。

导致 drupal 在处理 tar 压缩的文件时存在一处目录穿越漏洞，如果构造得当攻击者将获得 drupal 服务器控制权限。

pear Archive_Tar 在处理 tar 类型文件时未对符号链接进行严格校验导致目录穿越。

攻击者通过上传特制的 tar 类型文件，利用目录穿越漏洞可以上传 web shell 至 web 目录，并导致攻击者获得 drupal 服务器控制权限。

Archive_Tar 修复对比，也能发现主要针对符号链接进行了处理



五、 相关空间测绘数据

360 安全大脑-Quake 网络空间测绘系统通过对全网资产测绘，发现 Drupal 在全球 均有广泛使用，具体分布如下图所示。

六、 影响版本

产品名称	影响版本
Drupal	< 9.1.3
Drupal	< 9.0.11
Drupal	< 8.9.13
Drupal	< 7.78

七、 安全建议

(一) 通用修补方案

升级到最新版本:

- Drupal 9.1 版本用户，升级到 [Drupal 9.1.3](https://www.drupal.org/project/drupal/releases/9.1.3)

- Drupal 9.0 版本用户，升级到 [Drupal 9.0.11](https://www.drupal.org/project/drupal/releases/9.0.11)

- Drupal 8.9 版本用户，升级到 [Drupal 8.9.13](https://www.drupal.org/project/drupal/releases/8.9.13)

- Drupal 7 版本用户，升级到 [Drupal 7.78](https://www.drupal.org/project/drupal/releases/7.78)

(二) 临时修补方案

禁止用户上传 .tar、.tar.gz、.bz2 或.tlz 文件。

八、 产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

九、 参考链接

1. Drupal 官方通告

   https://www.drupal.org/sa-core-2021-001

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危