预警编号：YJ-2018012

恒安嘉新

关于 Drupal Core 远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 4 月 27 日

1 漏洞描述

近期，互联网爆出 Drupal Core 远程代码执行漏洞（CVE-2018-7602）。综合利用上述漏洞，攻击者可实现远程代码执行。部分漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大。故恒安嘉新第一时间发布预警公告。该漏洞危害程度为高危(High)。目前，厂商已发布了漏洞修复补丁。

2 影响范围

受影响版本：

Drupal 7.x，Drupal 8.x

修复版本：

Drupal 7.59，Drupal 8.5.3，Drupal 8.4.8

注：据互联网某平台对该系统在全球的分布情况统计，全球系统规模约为 30.9 万，用户量排名前五的分别是美国（48.5%）、德国（8.1%）、法国（4%）、英国（3.8%）和俄罗斯（3.7%）。在我国境内分布较少（0.88%）。

3 漏洞原理

Drupal 是一个由 Dries Buytaert 创立的自由开源的内容管理系统，用 PHP 语言写成。Drupal 在业界常被视为内容管理框架，而与一般意义上的内容管理系统存在差异。

2018 年 3 月 29 日，CNVD 收录了 Drupal 6、Drupal 7 及 Drupal 8 多

个子版本存在的远程代码执行漏洞，远程攻击者可利用该漏洞执行任意代码（http://www.cnvd.org.cn/webinfo/show/4463）。因 Drupal 官方对该漏洞修复不完全，导致补丁可以被绕过，任意代码被执行。过程如下：

Drupal 官方发布的漏洞补丁通过过滤带有＃的输入来处理请求数据（GET，POST，COOKIE，REQUEST），但 Drupal 应用还会处理 path?destination=URL 形式的请求，发起请求需要对 destination=URL 中的 URL 进行编码，攻击者对 URL 中的#进行两次编码即可绕过 sanitize()函数的过滤，从而实现远程代码执行。

4 修复建议

目前，厂商已发布了最新版本修复了漏洞，具体如下：

1）Drupal 7.x 需升级到 Drupal 7.59 版本。

官方给出 7.X 版本补丁，若用户无法立即升级版本，需更新补丁，补丁地址为：

https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=080daa38f265ea28444c540832509a48861587d0

2）Drupal 8.5.x 需升级到 Drupal 8.5.3 版本。

官方给出 8.X 版本补丁，若用户无法立即升级版本，请更新补丁，补丁地址为：

https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=bb6d396609600d1169da29456ba3db59abae4b7e

3）Drupal 8.4.x 版本需升级到 8.4.8 版本，官方给出 8.X 版本补丁，若用户无法立即升级版本，请更新补丁，补丁地址为：

https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=bb6d396609600d1169da29456ba3db59abae4b7e