预警编号：YJ-2018009

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 3 月 30 日

1 漏洞描述

近期，互联网爆出 Drupal core 远程代码执行漏洞（CVE-2018-7600）。综合利用上述漏洞，攻击者可实现远程代码执行攻击。目前，漏洞利用代码尚未公开。该漏洞危害程度为高危(High)。

2 影响范围

Drupal 的 6.x，7.x 和 8.x 版本受此漏洞影响。

据该系统在全球的分布情况的统计，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%），而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。在业界 Drupal 常被视为内容管理框架，而非一般意义上的内容管理系统。

Drupal 6，7，8 多个子版本存在远程代码执行漏洞，远程攻击者可利用该漏洞执行任意代码，从而影响到业务系统的安全性。

4 修复建议

目前，厂商已发布补丁和安全公告以修复该漏洞，具体修复建议如下：

1）推荐更新

主要支持版本推荐更新到 Drupal 相应的最新子版本。

7.x 版本更新到 7.58

更新地址：https://www.drupal.org/project/drupal/releases/7.58

8.5.x 版本更新到 8.5.1

更新地址：https://www.drupal.org/project/drupal/releases/8.5.1

8.4.x 版本更新到 8.4.6

更新地址：https://www.drupal.org/project/drupal/releases/8.4.6

8.3.x 版本更新到 8.3.9

更新地址：https://www.drupal.org/project/drupal/releases/8.3.9

2）使用 patch 更新

如果不能立即更新，请使用对应 patch。

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=2266d2a83db50e2f97682d9a0fb8a18e2722cba5

3）其他不支持版本

Drupal 8.0/8.1/8.2 版本已彻底不再维护，如果还在使用这些版本的 Drupal，请尽快更新到 8.3.9 或 8.4.6 版本。

Drupal 6 也受到漏洞影响，此版本由 Drupal 6 Long Term Support 维护。

参考链接： https://www.drupal.org/project/d6lts