ERT Threat Alert
Drupalgeddon 2
April 4, 2018

Abstract

Last week Drupal announced a critical vulnerability affecting Drupal version 7 and 8. Drupal is an open source content management software (CMS) written in PHP with almost a million users worldwide. The critical vulnerability in Drupal's CMS known as CVE-2018-7600[1] is a Remote Code Execution vulnerability that allows an attacker the ability to inject malicious code into vulnerable sections of Drupal. Drupal has published a pre-announcement and a security advisory, sa-core-2018-002[2], which describes the vulnerability and recommended steps for system administrators. Drupal urges administrators to perform the necessary updates to minimize the window of opportunity provided to cyber criminals. Attackers are now capable of developing exploits in the same day that a vulnerability is disclosed.

One issue encountered with the pre-announcement was that a large number of administrators were waiting for the release window to open, between 6:00pm and 7:30pm UTC. As a result, a large number of administrators attempted to download the updates at once, resulting in a flood that overwhelmed Drupal servers. Drupal has released a patch for version 8 and 7, which is available on the Drupal website.

Background

Content management systems are often targeted by attackers due to the large number of users who are dependent on their services and the data they hold. Because of this threat model and high rate of exposure, services like WordPress and Drupal are very quick about updating and securing their systems. Often times they pre-announce the update to allow administrators the time to schedule updates accordingly, but are often ignored, leaving a large surface area for cyber criminals to target.

In 2014, a critical vulnerability (CVE-2014-3704[3]) affecting Drupal version 7.x, prior to 7.32, was reported and patched promptly. This vulnerability in Drupal's API allowed attackers to send specially crafted requests that resulted in arbitrary SQL execution on targeted systems. This vulnerability was ultimately named Drupalgeddon due to its critical impact on Drupal users around the world. In the following years, there was a number of servers compromised because their administrators had failed to update their systems in a timely fashion.

The current vulnerability, CVE-2018-7600, has been named Drupalgeddon2 due to the critical impact on users. The fallout of Drupalgeddon in 2014 still lingers over this current disclosure as most security experts a week later are worried that once again a large number of administrators will fail to update their servers and fall victim to an attack the could have been prevented.

Attack Methods

The vulnerability affecting Drupal versions 7 and 8 is a remote code execution in multiple subsystems of Drupal's CMS. A remote attacker can construct a request with malicious content to exploit this vulnerability. A successful exploitation may lead to remote code injection of a Drupal server, which may lead to the server becoming completely compromised. Remote code execution attacks, or the execution of malicious code or commands on a target machine to extract sensitive information and/or abuse system functionality, may result in full control of the server.

Reasons for Concern

The reason for concern is the time it takes for system administrators to patch their Drupal servers. In 2014, a large number of sites suffered attacks from CVE-2014-3704 (Drupalgeddon) due to a failure to patch their servers. Drupal has released an update and given admins plenty of time to prepare for the critical update. If users do not update their Drupal servers, they can expect attackers to target their systems with remote code injection attacks in an attempt to fully compromise their system. As a result, an attacker can gain access to sensitive information and abuse system functionality.

---

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7600
[2] https://www.drupal.org/sa-core-2018-002
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704

During this window of opportunity, attackers can quickly create exploit scripts to target servers that have not been updated. Radware has witnessed this behavior that results in the creation of a botnet on the same day a vulnerability is published. Those that do make that update risk being exposed to threats.

Recommendations

Radware's recommendation is to upgrade to the patched release most closely related to your current version as per Drupal's recommendation. Upgrade to the most recent version of Drupal 7 or 8. If you are running 7.x, upgrade to 7.58 or if you are running 8.5.x, upgrade to Drupal 8.5.1.

For additional information:

- https://www.drupal.org/sa-core-2018-002
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7600

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.