NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

DRUPAL UNAUTHENTICATED REMOTE CODE EXECUTION VULNERABILITY CVE-2018-7600

DISCUSSION:

Drupal®[1] is a web-based Content Management System (CMS) written in PHP and commonly deployed using web servers such as Apache®[2] or Nginx®[3]. Use Body Text for most text in the template. This style has built in spacing.

On March 28, 2018, the Drupal project announced that a vulnerability had been discovered in Drupal 7.x and 8.5.x (as well as prior, unsupported versions) that allows an unauthenticated attacker to execute arbitrary commands on Drupal installations. In some situations, Drupal installations not directly connected to the Internet could be vulnerable to exploitation through a Cross-Site Request Forgery (CSRF) attack.

Web-based applications, such as Drupal, can be overlooked in routine patching since vulnerability scans may be unaware of their presence. Furthermore, administrators often postpone major version updates to web applications due to the frequent user impact and incompatibility with customized features. Web applications are a frequent target for attackers and vulnerabilities can be exploited days or even hours after their release. In general, configuring web applications to update automatically whenever possible is imperative for security.

There are many web-based CMSs similar to Drupal. Other common CMSs include Wordpress®[4] and Joomla®[5]. Organizations should be aware of CMS installations within their purview and ensure adequate processes are in place for timely updates.

MITIGATION ACTIONS:

System owners are advised to update to the latest version of Drupal, 8.5.1, which is not impacted by CVE®[6]-2018-7600. The Drupal project currently supports two major releases, Drupal 7 and Drupal 8.5. Installations of Drupal 7 should upgrade to 7.58. Other unsupported, outdated releases are not secure and should be immediately upgraded to Drupal 8.5.1. Compromised Drupal installations should be restored to a known good state before updating. Administrators should refer to the Drupal security advisory, SA-CORE-2018-002, for more information.

In addition, consideration should be given to implementing a Web Application Firewall (WAF) if one is not currently in place. The core WAF ruleset may block most attempts to exploit this Drupal vulnerability. In general, WAFs provide significant benefits to web application security and should be implemented in most environments.

APPLICABILITY:

This Bulletin is issued under the authority defined in National Security Directive 42 and applies to all Executive Departments and Agencies, and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in CNSS 4009.

[1] Drupal is a registered trademark of Dries Buytaert

[2] Apache is a registered trademark of the Apache Software Foundation

[3] Nginx is a registered trademark of Nginx Software Inc.

[4] Wordpress is a registerd trademark of the Wordpress Foundation

[5] Joomla is a registered trademark of Open Source Matters, Inc.

[6] CVE is a registered trademark of The MITRE Corporation

DISCLAIMER OF WARRANTIES AND ENDORSEMENT:

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

For further information about this product, please contact:
Client Requirements or General Cybersecurity Inquiries
Cybersecurity Requirements Center
410-854-4200
Email: Cybersecurity_Requests@nsa.gov