亚信安全紧急发布 Deep Security 安全更新，应对微软零日漏洞

近日 WordPress 曝出内容注入漏洞，随后微软曝出零日漏洞 CVE-2017-0016，截至目前微软并没有发布针对该漏洞的补丁程序，亚信安全紧急发布 Deep Security 安全更新，有效阻止上述漏洞。

- **漏洞名称：**
  CVE-2017-0016—微软 windows 堆栈溢出远程代码执行漏洞

  漏洞描述：
  该漏洞可以导致系统遭受远程拒绝服务攻击（DoS）。目前微软还没有发布补丁程序。

  解决方案：
  亚信安全 Deep Security 产品最新发布的入侵防御规则有效阻止该漏洞，请用户及时更新应用规则。

- **漏洞名称：**
  WordPress REST API 内容注入漏洞

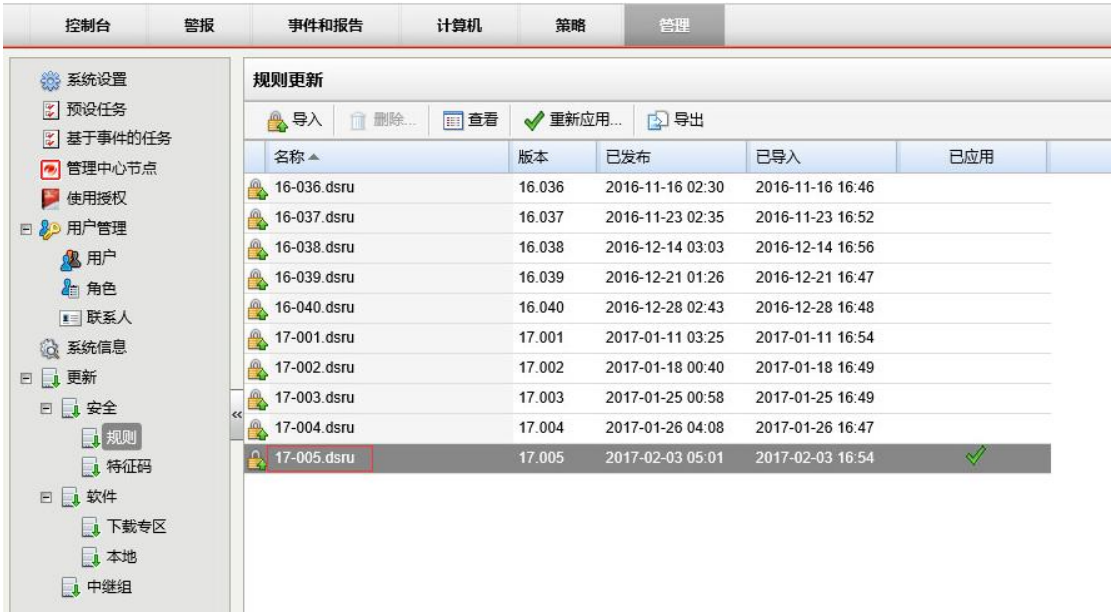
  漏洞描述：
  攻击者利用该漏洞可在 WordPress 搭建的网站注入恶意内容，提升权限，对文章、页面等内容进行修改。

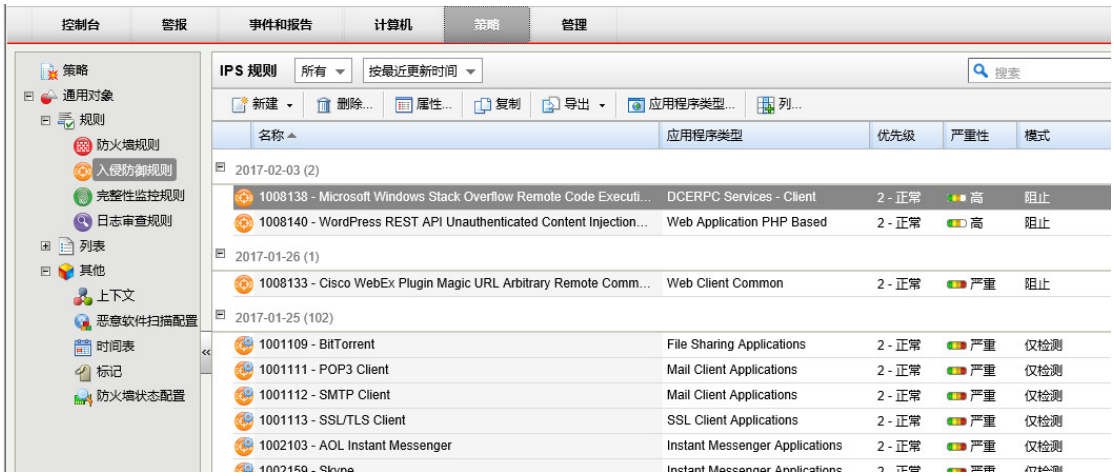
  影响版本：
  WordPress 4.7.0 – WordPress 4.7.1

  解决方案：
  ①升级到 WordPress 4.7.2 版本
  ②亚信安全 Deep Security 产品最新发布的入侵防御规则有效阻止该漏洞，请用户及时更新应用规则。

针对上述漏洞，亚信安全紧急发布 Deep Security 安全更新，DSRU ID : 17-005，本次更新包含的具体规则内容如下：

1008138-Microsoft Windows Stack Overflow Remote Code Execution Vulnerability
1008140-WordPress REST API Unauthenticated Content Injection Vulnerability





亚信安全服务器深度安全防护系统(Deep Security)提供了一种全方位服务器安全平台，旨在保护用户的数据中心和云平台免遭数据泄露和业务中断，并降低运营成本。可以以多种方式组合使用的模块包括防恶意软件、Web 信誉、防火墙、入侵阻止、完整性监控和日志检查，以确保物理、虚拟和云环境中服务器的应用程序以及数据的安全。其中入侵检测和阻止模块具有如下功能：

- 屏蔽已知漏洞以防止其被无限制利用，进而防止已知攻击和零日攻击的入侵
- 检查所有传入及传出通信，不允许协议修改、违反策略和可能导致攻击的内容无机可乘
- 几小时内便可自动屏蔽新发现的漏洞，只需几分钟即可以将防护推送至数千台服务器，且无需重启
- 防止 SQL 注入、跨站点脚本攻击和其他 Web 应用程序漏洞
- 在代码修复完成之前屏蔽漏洞

- 为所有主要的操作系统和超过百款应用程序（包含数据库、Web 服务器、电子邮件服务器和 FTP 服务器）提供立即、可用的漏洞防护
- 更好地查看或控制访问网络的应用程序