

漏洞相关信息

漏洞编号: CVE-2012-2376、CVE-2015-4601、CVE-2014-9427、CVE-2013-6420、CVE-2013-1635、CVE-2016-7411、CVE-2016-6288、CVE-2011-4718、CVE-2012-5381、CVE-2012-1172等  
漏洞名称: PHP  
产品型号及版本: ComwareV7 防火墙、负载均衡、IPS产品

漏洞描述

PHP 'com\_print\_typeinfo'函数缓冲区溢出漏洞(CVE-2012-2376)  
PHP "crypt()" MD5 Salt安全漏洞  
PHP多个内存破坏漏洞 (CVE-2015-4601)  
PHP '\_php\_stream\_scandir()'缓冲区溢出漏洞  
PHP-CGI远程任意代码执行漏洞  
PHP 'cgi\_main.c'越界读拒绝服务漏洞(CVE-2014-9427)  
PHP 'phar/tar.c'数字错误漏洞  
PHP OpenSSL Extension 'openssl\_x509\_parse()'内存破坏漏洞(CVE-2013-6420)  
PHP "substr\_replace()"释放后重用远程内存破坏漏洞  
PHP 任意代码执行漏洞  
PHP 'QUERY\_STRING' 参数安全漏洞  
PHP 任意文件泄露和任意文件写漏洞(CVE-2013-1635)  
PHP ext/sockets/sockets.c socket\_connect函数栈缓冲区溢出漏洞  
PHP 内存损坏漏洞(CVE-2016-7411)  
PHP "shmop\_read()"远程整数溢出漏洞  
PHP"phar/phar\_object.c"格式字符串漏洞  
PHP php\_url\_parse\_ex拒绝服务漏洞(CVE-2016-6288)  
PHP "magic\_quotes\_gpc"指令安全限制绕过漏洞  
PHP ext/xml/xml.c 拒绝服务漏洞  
PHP Sessions子系统会话固定漏洞(CVE-2011-4718)  
PHP main/rfc1867.c rfc1867\_post\_handler函数文件路径注入漏洞  
PHP libxslt安全限制绕过漏洞 PHP 5 cron job任意文件删除漏洞  
PHP 不安全文件权限漏洞(CVE-2012-5381)  
PHP目录遍历漏洞 (CVE-2012-1172)  
PHP "Intl"扩展"NumberFormatter::setSymbol()"函数拒绝服务漏洞  
PHP资源管理错误漏洞 PHP Web表单哈希冲突拒绝服务漏洞  
PHP PDORow对象远程拒绝服务漏洞  
PHP 5.3.9之前版本strtotime函数调用远程拒绝访问漏洞  
PHP栈缓冲区溢出漏洞(CVE-2010-4698)  
PHP 5.3.7之前版本多个漏洞  
PHP 'cdf\_read\_property\_info()'函数拒绝服务漏洞 (CVE-2014-0238)  
PHP 安全漏洞(CVE-2017-11143)  
PHP Fileinfo组件拒绝服务漏洞  
PHP 资源管理错误漏洞 (CVE-2014-0237)  
PHP 'tidy\_diagnose'函数拒绝服务漏洞  
PHP 'SQLite'功能权限许可和访问控制漏洞  
PHP 'libxml RSHUTDOWN'函数信息泄露漏洞  
PHP 'zend\_strndup()' 拒绝服务漏洞  
PHP SOAP解析器信息泄露漏洞 (CVE-2013-1643)  
PHP Calendar SdnToJulian函数整数溢出漏洞  
PHP 安全漏洞 (CVE-2016-7478)  
PHP "ZipArchive::addGlob"和"ZipArchive::addPattern"资源管理错误漏洞  
PHP 'sapi/cgi/cgi\_main.c' SQL注入漏洞  
PHP拒绝服务漏洞 PHP ICU Intl grapheme\_extract函数任意代码执行漏洞  
PHP GD组件拒绝服务漏洞  
PHP 基于堆的缓冲区溢出漏洞 (CVE-2013-2110)  
PHP 'odbc\_bindcols'函数安全漏洞  
PHP 代码注入漏洞 PHP SSL Certificate Validation 安全绕过漏洞  
PHP Exif扩展exif.c拒绝服务漏洞  
PHP crypt函数加密问题漏洞  
PHP Streams组件拒绝服务漏洞  
PHP Zip扩展\_zip\_name\_locate函数拒绝服务漏洞

PHP strval函数缓冲区溢出漏洞  
PHP OpenSSL扩展多个内存泄露漏洞  
PHP SOAP解析器信息泄露漏洞 (CVE-2013-1824)  
PHP Zip扩展拒绝服务漏洞 可能存在CSRF攻击  
PHP Pear '/tmp/Directory' 安全漏洞(CVE-2014-5459)  
PHP 安全漏洞(CVE-2014-4721)

#### 漏洞解决方案

Comware v7产品均不涉及此漏洞。

