
# 安全威胁每周警讯

2011/08/14～2011/08/20

本周威胁指数


***TrendMicro* 中国区网络安全监控中心**


# 前十大病毒警讯

| 排名 | 病毒名称 | 威胁类型 | 风险等级 | 趋势 | 病毒行为描述 |
|---|---|---|---|---|---|
| 1 | TROJ_DOWNAD.INF | 木马 | ★★★ | → | DOWNAD 蠕虫关联木马 |
| 2 | WORM_DOWNAD.AD | 蠕虫 | ★★★★ | → | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| 3 | TROJ_IFRAME.CP | 木马 | ★★★ | ↑ | GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序 |
| 4 | WORM_DOWNAD | 蠕虫 | ★★★★ | ↓ | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| 5 | Cryp_Xed-12 | 木马 | ★★★ | → | 木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染 |
| 6 | CRCK_KEYGEN | 破解程序 | ★★ | ↑ | 非法破解程序 |
| 7 | JS_EXPLOIT.SMAD | 木马 | ★★★ | ↑ | 这是使用趋势科技智能检测功能所检测出的疑似 Java 脚本病毒程序 |
| 8 | PAK_Generic.001 | 木马 | ★★★ | → | 加壳程序，疑似病毒文件 |
| 9 | WORM_ECODE.E-CN | 蠕虫 | ★★★★ | ↓ | E 语言病毒,产生与当前文件夹同名 exe 文件 |
| 10 | TROJ_SPNR.03CG11 | 木马 | ★★★ | ↑ | 木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染 |

# 系统漏洞信息

## 1.1. MS11-069：.NET Framework 中的漏洞可能允许信息泄露 (2567951)

Windows XP

Windows Vista

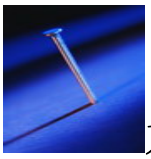
Windows 7

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

**描述：**http://www.microsoft.com/china/technet/security/bulletin/MS11-069.mspx



# 系统安全技巧

你的 SSL 服务器是否存在着错误的配置和已知的漏洞?这些不安全的因素会给企业网络带来极大的安全风险。遵循下面这些技巧可以使你避免一些常见的 SSL 安全错误，让你远离风险。

**1、 禁用对 SSLv2 的支持。**

该版本的 SSL 协议在 15 多年前就被证明是不安全的，但如今有许多 Web 服务器仍在使用它。

禁用此协议用了不多少时间。例如，在 Apache v2 中，你需要对默认为配置进行改变：

将：SSLProtocol all

变为：SSLProtocol all -SSLv2

**2、 禁用对弱加密的支持。**

几乎所有的 Web 服务器都支持强加密算法(128 位)或极强的加密算法(256 位)，但许多服务器还在支持弱加密，黑客们会利用这个漏洞来损害企业网络安全。我们没有理由支持弱加密，只需用很短的时间来配置服务器就可以禁用弱加密：

SSLCipherSuite RSA:!EXP:!NULL:+HIGH:+MEDIUM:-LOW

**3、确保你的服务器不支持不安全的重新会话。**

SSL 和 TLS 认证中的漏洞可以使中间人攻击利用重新会话，将任意内容插入到加密的数据流中。如今，多数主要的厂商都为此漏洞发布了补丁，所以如果你还没有打补丁，就必须实施安全的重新会话，或者至少禁用不安全的重新会话(对网站作出任何必要的改变)。

**4、确保所有的认证阶段都通过 SSL 进行。**

保护用户凭证至关重要，而这意味着在用户提交表单时，你需要通过 SSL 连接发送用户登录的表单，并且借助 SSL 来保护其凭证。否则，就有可能被黑客截获表单，并用一个别有用心的不安全表单来替换之，进而将用户的凭证发送到黑客自己的服务器上。

**5、不要在网页上将 SSL 保护的内容与明文混在一起。**

将二者混在一起会导致网站遭受损害，因为一个不受保护的源(如 JavaScript)可被用于注入恶意代码，或导致中间人攻击。

**6、使用 HSTS 协议来保护域名(包括子域)。**

在用 HSTS 保护网站时，在初次访问后，到网站的所有链接都会自动地从 HTTP 转换为 HTTPS，而且访问者无法再次访问网站，除非它拥有一个合法的、并非自己签名的数字证书。这意味着黑客们无法将用户重向到钓鱼网站(黑客通过一个不安全的链接来控制此网站或窃取不安全的会话 cookies)。

必须只能通过 HTTPS 的应答来发送严格传输安全(STS)的报头，并且只需简单的几行就可以搞定其配置。对于 Apache 而言，可以这样操作：

Header set Strict-Transport-Security "max-age=XXXXXX"

Header append Strict-Transport-Security includeSubDomains

**7、使用 HttpOnly 和 Secure 标记来保护 cookies**

用于认证的 cookies 在 SSL 会话期间可被用于损害会话的 SSL 安全性。HttpOnly 标记可以使你发布的 cookies 对客户端脚本不可见，所以客户端无法通过跨站脚本攻击漏洞来窃取 cookies，而 Secure 标记意味着，只能通过一个加密的 SSL 连接来传输 cookies，因而 cookies 无法被截获。

为了配置你的 web 服务器，使其能够通过 HttpOnly 和 Secure 属性来发布 cookies 从而防护这两种攻击，你只需要简单地增加将; Secure ; HttpOnly 添加到 Set Cookie Http 响应报头中：

Set-Cookie: =; =

; expires=; domain=

; secure; HttpOnly

**8、使用扩展验证(EV)的数字证书。**

虽然对于网站的安全并非生死攸关，但扩展验证证书却可以在多数浏览器的地址栏中得到清晰的证实，即访问者拥有了一个到达网站的安全的 SSL 连接。只有在认证授权采取了严格的措施来确认你的身份后，并且是你控制着发布证书的域名时，才会发布扩展验证证书。

**9、确保你的数字证书包括子域**

为避免访问者收到数字证书错误，一定要保证你的SSL证书覆盖https://www.贵站域名.com和https://贵站域名.com这两个URL。

你可以使用一个多域的SSL证书来实现此功能，这种证书通常会允许你指定多达三个主题选择名称(即SAN)，如贵站域名.com或者www.贵站域名.com

来源：IT168