安全威胁每周警讯

2012/03/25～2012/04/01

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	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
2	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
3	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 蠕虫关联木马
4	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
5	JS_SCRIPT.JDR	脚本病毒	★★	↑	该病毒为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。
6	JS_MALAGENT.CEO	脚本病毒	★★	↑	该病毒为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。
7	SWF_EXPLOIT.JWE	脚本病毒	★★	↑	该病毒为 flash 脚本病毒，通常是用户访问恶意网站上的 flash 文件感染。
8	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
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	JS_AGENT.BBCK	脚本病毒	★★	↑	该病毒为 Java 脚本病毒，通常是用户访问恶意网站是所感染的。

系统漏洞信息

MS12-011 ： Microsoft SharePoint 中的漏洞可能允许特权提升 (2663841)

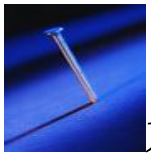
Microsoft SharePoint Server 2010

Microsoft SharePoint Server 2010 Service Pack 1

Microsoft SharePoint Foundation 2010

Microsoft SharePoint Foundation 2010 Service Pack 1

描述： http://technet.microsoft.com/zh-cn/security/bulletin/MS12-011



系统安全技巧

对企业而言，执行信息安全漏洞分析是一项非常有利的操作，但它很少被正确执行。首先，企业必须先了解执行信息安全漏洞分析的目的，然后才能进一步证明它是有用的。网络漏洞分析是根据已证明的标准来审查网络，从而确定哪些关键区域需要改进。

企业应使用网络安全漏洞分析来查找其网络上的漏洞，同时帮助发现需要注意的地方。安全小组可能、或不可能已经认识到被发现的漏洞，但该过程(指进行安全漏洞分析)为发现和解决网络安全问题提供了一个机会，并以最小的工作量去修补问题;同时，它以一个正式的方式为高层管理人员展现了更多复杂的、突出的问题。

当执行网络漏洞分析时，企业需要一个基准去比较其各个环境，常用基准是一个或多个组织或行业的标准或法规。现在有很多这样的框架，其中的一些是规定，比如支付卡行业数据安全标准(PCI DSS)，而其他的则是关于如何运用标准和最佳业务实践的好例子，比如来自美国国家标准与技术研究院(NIST)的内容。很少有企业能够完全彻底地符合任何标准，应该利用在分析中所发现的漏洞，以确定需要解决的领域和日后需要重点关注的地方。如果选择的框架并不涵盖一切需要，企业可以结合不同标准的其他方面来创建一个初始的基准。根据你的行业和你的环境，很难找到一个框架将完全满足你的所有需求。使用一个标准为基准，连同其他不同的基准控制是完全正常的。管理员必须自己判断他们应该在分析中输入什么内容。大多数框架将非常有效，但这取决于你最后所决定的框架的最终样子。这是一个颇具权威的起点，但企业还是应该选择适合自己独特标准和业务目标的控制。这并不意味着不能改变，但在你的分析开始之前，你应该试试并确定你的框架。

一个漏洞分析可划分为四个主要领域：政策和程序，审计，技术审查和调查结果/优先级汇总。上述四个阶段进行如下。

信息安全漏洞分析第 1 步：政策和程序

在这个初始阶段，企业需根据其网络安全策略审查应用于网络的所有书面或电子形式的程序。更糟的是网络文件共享中的陈旧政策，它们未被修订和使用。移除不需要的，更新当前的，删除旧的，同时以书面形

式添加任何新的政策。如果网络安全政策没有被定期审核，那么对企业来说它们就绝对是无用的。

这样的例子是显而易见的，比如当你网络上的防火墙改变时。改变时，你的策略是什么？谁可以对你网络上的防火墙进行更改？企业需要注意的政策的要求更换;管理需要理解审批程序，而管理员需要有标准作业程序来合理地完成变化。

信息安全漏洞分析第 2 步：审计

漏洞分析的第二阶段是审计，其中包括审查带有不断更新政策和程序的框架。此外，通过运用框架标准，验证企业是否遵循自己的政策。分析不仅是一个技术问题，而是一个人的问题。例如，工程师们需要注意当改变防火墙时要遵循的政策，他们必须输入适当的变更管理票并审查。

例如，当审计防火墙上开放的端口时，企业应该能够为每个端口显示所有适当的变更控制票(changecontrol tickets)。当防火墙里的一个空穴没有变更控制时，这就是一个漏洞，在技术和程序上都需要填补。选定的框架所协助的端口应该是开放的，然后考虑到框架，通过审查网络，企业可以得出结论，看是否有漏洞需要修补。还是用防火墙的例子，如果入站防火墙中的端口 3389 被打开了，首先要确定应对这种变化的合适的变更控制。这有助于审计程序。接着，使用选定的框架再进一步审查，并确定这个入站端口被打开是安全漏洞还是违反企业标准。这就是如何将审计程序和政策框架联系在一起。

信息安全漏洞分析第 3 步：技术审查

漏洞分析的第三个阶段是网络的技术审查。这个阶段与审计阶段是紧密结合的，但比起政策和程序，它更依赖于框架。在审计阶段，企业需要政策和程序，并针对它们应用框架以确保符合新的标准。在技术审查阶段，企业验证其技术基础设施是否是最新的架构，并考察系统安全的粒度级别。在网络上应用框架，以确定框架是否符合标准。例如，如果一个框架的状态是 IPS 被安装在出站过滤防火墙上，企业应验证这样是否正确。如果不正确，企业需要用技术来填补这些在其网络上的漏洞。

这是为了验证相应的技术控制是否到位。最终这又与审计联系到一起，但框架必须首先达到标准。问问这样的问题：企业在所有的服务器上都使用了杀毒软件吗？是否有漏洞管理？在数据库上使用了加密吗？这些都是一些控制例子，用于比较框架是否落实到位。这为企业提供了清晰的了解，并使企业可以掌握哪些地方累加了当前的标准。

信息安全漏洞分析第 4 步：结果和优先级汇总

最后，第四阶段是审查结果和新任务的优先次序。这个阶段中，企业要审查其他阶段的结果，评价发现了什么，并安排任务来修复漏洞。包括与管理人员见面、访问需要的任何人，以获取更多信息。还包括解决政策和程序中的漏洞，讨论需立即进行的可能修复、以及为满足现有基准在技术上需要什么到位。

适当的优先级也应该出现在所有这些阶段。为消除这些漏洞，这个领域需要讨论和解决。最后，企业应定期运行漏洞分析，从而确保它不会倒退、或回到过去的坏习惯。应该有一个关于需要改进的地方的运行列表。这个列表可以由审计团队编写，当他们在计划的漏洞分析间做现场审计时。一旦发现异常，应审查特定区域的框架。企业的目标是拥有一个始终如一的一致性框架，而不是每年都需要清理。当这些问题被发现，

应立即修复或引起高层管理人员的注意。

结论

请记住，进行网络安全漏洞分析并不是一件容易的事情，它可能需要很长的时间去符合企业的选定框架标准。进行分析时，企业可能会有一些令人不快的发现(如发现很多漏洞)，但这正是进行分析的目的。最终的目标是，保护企业免受那些故意伤害，这意味着，企业需要在攻击者发现之前发现那些问题。

来源：比特网