

Novell eDirectory iMonitor “Accept-Language”头溢出漏洞

漏洞报告

发布日期

2009年03月03日 09:52:57 AM

版本 5

更新标题，简述及分析部分

过去的版本

名字	版本号	版本注释	发布日期
Novell eDirectory iMonitor “Accept-Language”头溢出漏洞	4	添加验证漏洞代码 DirServer_iMonitor_DoS.pl	2009年02月02日
Novell eDirectory iMonitor “Accept-Language”头溢出漏洞	3	更新简述内容	2009年02月02日
Novell eDirectory iMonitor “Accept-Language”头溢出漏洞	2	更新受影响产品信息	2009年02月02日
Novell eDirectory iMonitor “Accept-Language”头溢出漏洞	1	添加资源信息	2009年01月27日

简介

风险等级：中

解决方案：补丁

利用后果：代码执行

漏洞类型：off-by-one错误

利用途径：本地网络访问；Web

文档编号：094964

报告

综述：

所有的 off-by-one 漏洞都存在于 Novell eDirectory 8.8 SP3 的 iMonitor

“Accept-Language”头处理中，一旦此漏洞被利用，将允许攻击者远程执行任意代码。用户需要知道其验证代码已经公开。建议安装官方补丁解决此问题。

简述：

Novell eDirectory是X.500 兼容的目录服务的软件产品，用于在某一特定的网络集中管理获取资源的多服务器和计算机。eDirectory的iMonitor组件是一个在所有服务器的eDirectory树中跨平台的监测和诊断实用工具。它允许通过监听TCP 8028 端口通过web服务器远程监控。

“Accept-Language”是为RFC2616的HTTP/1.1 中 14.4 段定义的一个可选HTTP报头，通常被用来声明代表用户接收文件语言偏好。“Accept-Language”的格式如下：

Accept-Language: [language-tag];[optional quality value], [language-tag];[optional quality value], ...

语言标记是一个符合接受语言代码ISO-639-1和ISO 3166-1 标准的值。例如, 'en'是英文编码, 而'en-gb'则进一步被归类为英国英语编码。

iMonitor处理HTTP报头"Accept-Language"时存在漏洞。使用前没有正确地执行边界检查。具体来说, 当用户请求处理超过20个语言标签的时候导致错误。下面的代码显示了此漏洞:

```
.text:635D426A      cmp             ebx, 14h
.text:635D426D      jg             loc_635D43CB
```

此代码检查该指数是否(存储在寄存器ebx)大于0x14(十进制的20)。如果是, 则跳出循环。如果小于或等于20, 则继续处理用户请求的值。因为index0引用数组中的头一个元素, 所以index20将引用数组的第21个元素。由于数组只能容纳20个元素, 所以无论存储在这个index的数据将被重写。补丁代码检查index是否大于或等于0x14, 以解决off-by-one漏洞。

分析:

攻击者可以利用此漏洞在目标系统中执行任意代码。攻击者将利用恶意"Accept-Language"报头构造 HTTP/1.1 包。此恶意报头包文件含有根据需求定制的 20 个可被接受的语言, 且第 20 条带有 payload。攻击者将发送这些恶意请求给目标, 并默认监听 TCP8028 端口。由于第 20 条被写入超过最初分配的数组, 返回地址可能会被部分重写。

成功利用此漏洞可以在受影响系统上以管理权限执行任意代码。利用失败则会导致应用程序崩溃, 可能进入多个网络资源导致拒绝服务。对于 Windows 版本的 eDirectory 8.8 SP3 的缓解条件是, 防止堆栈的 Cookie 覆盖返回地址栈, 阻碍执行任意代码。但是, 用户应该了解其他版本或其他平台可能仍然容易受感染导致任意代码执行。进一步减轻的因素是, 通常这种应用不直接从外部提供的网络防火墙。

一个被设计成导致应用程序崩溃的验证代码被发布在Milw0rm网站上。iSIGHT Partners测试了此代码后发现对eDirectory 8.8 SP3 的Windows版本无效。发布的验证代码指向了错误的TCP端口, 8008, 但是当指向正确的端口时, 仍然无效。这表明, 验证代码作者使用的测试系统可能使用默认设置, 或针对旧版本的, 如 8.7.3 的旧版本eDirectory, 如果TCP 80 已经在使用中使用TCP端口 8008。此问题应当指出, 然而, iSIGHT Partners实验室能够修改此验证代码在一个平凡的可靠触发该缺陷, 对于Windows版本可 100%导致应用程序崩溃。

Novell 公司为 eDirectory 8.8 SP3 发布了补丁 FTF3 以解决这一问题。iSIGHT Partners 不知道其他解决此漏洞的方式。

这个安全漏洞的风险部分取决于网络内的位置。通常情况下, eDirectory 工作于内网络, 未暴露外部的流量。然而, 攻击者已经获得了内部主机通过不同的弱点可能会克服这个减轻关注。虽然 iSIGHT Partners 尚未确认代码执行的可能性, 拒绝服务攻击条件可能同样存在问题, 因为这将破坏所有客户的依赖的服务。鉴于公众提供 PoC 业务似乎是针对具体的目标, iSIGHT Partners 认为这是一个中等风险的漏洞。

受影响的产品:

iSIGHT Partners 已经确认 eDirectory 8.8 SP3 的 Windows 版本存在此漏洞。Novell 公司称 eDirectory 8.8 SP3 的 Linux, Unix, Windows and Netware 版本也存在此问题。此外, Assurent 称 Novell eDirectory 8.7.3 and 8.8.4 同样存在此漏洞。

解决方案:

除安装官方补丁之外, iSIGHT Partners 尚未发现其他方法。

官方补丁:

Novell 发布了补丁 FTF3 以解决此漏洞。有关此漏洞的详细信息和补丁程序, 可以从下列地址列表中获取:

[Novell eDirectory 8.8 SP3 FTF3 Linux/Unix Security Update Information](#)

[Novell eDirectory 8.8 SP3 FTF3 Netware Security Update Information](#)

[Novell eDirectory 8.8 SP3 FTF3 Windows Security Update Information](#)

TCP 端口:

8028

利用代码

文件名	文件大小	MD5 校验和	下载地址	有效性
DirServer_iMonitor_	1958	b4712aeecff6c82fe72	http://www.milw0	
DoS.pl	Bytes	d833f5af01e3f	rm.com/ exploits/8129	0%

参考资料

CVSS基本得分: 9.3 (AV:N/AC:M/AU:N/C:C/I:C/A:C) **CVSS时间分:** 7.3 (E:P/RL:O/RC:C)

BugTraq 编号: 33928

攻击难易度: 易

信息资源

名称	日期	网站地址	说明
Full-Disclosure	2009年02月27日	http://lists.grok.org.uk/pipermail/full-disclosure/2009-February/068160.html	VRSubscriptionnoreply@assurent.com, Assurent VR -Novell eDirectory iMonitor “Accept-Language”头溢出漏洞
IETF	2009年03月03日	http://www.ietf.org/rfc/rfc2616.txt	超文本传输协议 -- HTTP/1.1
Interna	2009年03月03日	http://www.iso.org/iso/english	英文国家名和代码

tion Organiz ation for Standar ds		_country_names_and_code_el ements	
Novell Inc.	2009年02月25日	http://support.novell.com/docs/Readmes/InfoDocument/patch_builder/readme_5042342.html	文档编号: 5042342
Novell Inc.	2009年02月25日	http://support.novell.com/docs/Readmes/InfoDocument/patch_builder/readme_5042341.html	文档编号: 504234
Novell Inc.	2009年02月25日	http://support.novell.com/docs/Readmes/InfoDocument/patch_builder/readme_5042340.html	文档编号: 5042340
Novell Inc.	2009年03月03日	http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/a5j35ef.html	iMonitor Architecture
US Library of Congre ss	2009年03月03日	http://www.loc.gov/standards/iso639-2/php/code_list.php	ISO 639 代码列表

技术支持

厂商	技术名称	网站地址
Novell Inc.	eDirectory 8.8 SP 3	
Novell Inc.	eDirectory 8.8 SP 4	
Novell Inc.	eDirectory 8.7.3	