

GHOST glibc 远程代码执行漏洞会影响所有的 Linux 系统

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	GHOST glibc Remote Code Execution Vulnerability Affects All Linux Systems		
原文作者	Michael Mimoso	原文发布日期	2015 年 1 月 27 日
作者简介	Michael Mimoso 是一名经验丰富的记者，拥有超过 15 年的网站、杂志和报纸的撰写和编辑经验。 www.linkedin.com/in/michaelmimoso		
原文发布单位	Threatpost		
原文出处	http://threatpost.com/ghost-glibc-remote-code-execution-vulnerability-affects-all-linux-systems/110679		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 		

- 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

GHOST glibc 远程代码执行漏洞会影响所有的 Linux 系统

Michael Mimoso

2015 年 1 月 27 日



Glibc (GNU C 库) 中发现了一个严重的漏洞, 该漏洞能够影响所有追溯至 2000 年的 Linux 系统。攻击者可以利用该漏洞来执行代码并远程控制 Linux 机器。

该漏洞源于 glibc 的函数 `__nss_hostname_digits_dots()` 的基于堆的缓冲区溢出。这一特殊的函数由 `_gethostbyname` 函数调用。

“远程攻击者能够调用这些函数的任意一个, 在获得运行该程序的用户的许可的情况下, 能够利用该漏洞执行任意代码”, Linux 发行商 Red Hat 的公告说。该漏洞被命名为 CVE-2015-0235, 由于其与 `_gethostbyname` 函数的关联被戏称为 GHOST。Qualys 公司的研究人员发现了该漏洞, 认为第一个被感染的 glibc 版本是 2000 年 11 月发布的 Linux 系统的 glibc2.2。

根据 Qualys, 2013 年 5 月 21 日 (介于 glibc-2.17 和 glibc-2.18 发布之间), 该问题的缓解方案被发布。

“不幸的是, 它没有被视为一个安全威胁; 其结果是, 最稳定的和长期发行的操作系统遭到了感染, 包括 Debian 7 (wheezy)、Red Hat Enterprise Linux 6 和 7、CentOS 6 和 7、

Ubuntu12.04 等”，Qualys 公司的公告这样说。

各个 Linux 发行版将会发布补丁；Red Hat 发布了 Red Hat Enterprise Linux v.5 服务器的更新。Novell 公司列出了被该漏洞感染的 SUSE Linux Enterprise Server 的列表。Debian 已经发布了解决该漏洞的软件更新。

“该漏洞随处可见，因此情况很紧迫。该漏洞已经感染 glibc 很长一段时间了。最近它被修复，但是没有被视为一个安全问题，所以较新的版本应该没问题”，Red Hat 安全响应团队的成员 Josh Bressers 这样说，“从威胁层面来看，该漏洞针对使用该函数的系统”。

不像过去的互联网范围的 bug(如 Bash)，修补 glibc 未必是件苦差事。“在这种情况下，你只要应用 glibc 更新，并重新启动任何有漏洞的服务”，Bressers 说，“它不像 Shellshock 那样令人迷惑”。

Qualys 公司不仅在公告中分享了极为深入的 GHOST 技术信息，还介绍了 Exim SMTP 邮件服务器的漏洞利用。该公告展示了如何绕过 NX（即 No-eXecute，不可执行）保护方案以及 glibc malloc 的硬化。

除了 2013 年的补丁，Qualys 公司还介绍了其它能够缓解该漏洞影响的因素，包括以下事实：由于 IPv6 和较新的应用使用不同的函数调用 `getaddrinfo()`，`gethostbyname` 函数已经过时了。虽然该漏洞也可本地利用，但是这种情况的可能性也大大降低了，原因是：只有在初步调用失败，二次调用成功的情况下，许多程序才会依靠 `gethostbyname` 实现溢出。公告说这是“不可能的”，所以那些程序是安全的。

Qualys 说，远程漏洞利用也有所缓解。例如，服务器使用 `gethostbyname` 来执行全周期反向 DNS 检查。“这些程序一般都是安全的，因为传递到 `gethostbyname()` 的主机名通常会由 DNS 软件预先验证”，该公告说。

“目前看来，这并不是一个很严重的远程问题”，Bressers 说。

虽然该漏洞可能自 2000 年以来一直处于休眠状态，但是我们无法确定罪犯或政府资助的黑客是否在利用该漏洞。该漏洞的信息已经公开，一旦合法的安全研究人员和黑客们开始进行研究，谁也没办法预测将会发生什么。在 Bash 的案例中，没过多久就出现了其他的安全问题。