

GHOST 漏洞

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	The GHOST Vulnerability		
原文作者	Wolfgang KandeK	原文发布日期	2015 年 1 月 27 日
作者简介	Wolfgang KandeK 是 Qualys 公司的首席技术官，负责 QualysGuard 平台的技术创新和市场推广。有 20 多年的信息系统开发和管理经验。 http://www.linkedin.com/in/wkandek		
原文发布单位	Qualys 公司		
原文出处	https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability?utm_source=tuicool		
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 		

	<p>权问题承担责任。</p> <ul style="list-style-type: none">• 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 漏洞

Wolfgang Kandek

2015 年 1 月 27 日

GHOST (幽灵) 漏洞是 Linux glibc 库的一个严重漏洞。它使得攻击者能够远程完全控制受害系统，而无需事先获取系统凭证。该漏洞被命名为 CVE-2015-0235。

Qualys 公司的安全研究人员发现了这个 bug (错误)，并与 Linux 发行商密切合作。通过协作，我们得以在今天发布此通报，补丁也于 2015 年 1 月 27 日发布。

Glibc 是什么？

Glibc (即 GNU C 库) 是 Linux 操作系统的标准 C 库实现和核心部分。如果没有这个库，Linux 系统将无法正常运作。

GHOST 漏洞是什么？

在代码审核中，Qualys 的研究人员发现了 glibc 的函数 `_nss_hostname_digits_dots()` 出现缓冲区溢出。此 bug 可以通过所有的 `gethostbyname*()` 函数本地和远程触发。应用程序主要通过 `gethostbyname*()` 函数集合访问 DNS 解析器。这些函数将主机名转换为 IP 地址。

更多细节可以参考 YouTube 采访视频。

风险如何？

该漏洞导致了远程代码执行风险。利用该漏洞的攻击者可以获取被感染系统的完全控制权。

真有这种风险？

在测试中，我们设计了一个概念验证，向邮件服务器发送特别创建的电子邮件，并可以得到 Linux 机器的一个远程 shell。这样能够绕过 32 位和 64 位系统的所有现有保护方案 (如 ASLR，PIE 和 NX)。

如何降低风险？

为了降低风险，最好的方法是采用 Linux 厂商的补丁。Qualys 公司已经与 Linux 发行商

紧密合作，补丁程序已于 2015 年 1 月 27 日发布。

为什么称为 GHOST 漏洞？

该漏洞能够被 GetHOST 函数触发，因此被称为 GHOST 漏洞。

这是一个设计缺陷？

不是的，这是被感染的软件版本的实现问题。

哪些版本和操作系统受到影响？

第一个受到影响的 GNU C 库是发布于 2000 年 11 月 10 日的 glibc-2.2。我们确定了一些缓解该 bug 影响的因素。特别是，我们发现，它在 2013 年 5 月 21 日（介于 glibc-2.17 和 glibc-2.18 的发布之间）被修复。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、Ubuntu 12.04 等。

哪里可以下载该漏洞？

我们希望给大家足够的时间进行修复。根据我们的数据，一旦该漏洞已经到达其半衰期，我们将会发布该漏洞。半衰期是指漏洞出现量减半所需要的时间。随着时间的推移，这个指标显示了消除漏洞的举措效果如何。较短的半衰期意味着更快的恢复。半衰期一词最初是由 Qualys 公司在“漏洞原理”板块使用的。

Qualys 的客户可以用 Qualys Vulnerability Management 云解决方案（即 QID123191）来检测 GHOST 漏洞。这意味着 Qualys 的客户可以得到其企业受影响程度的报告，从而了解 GHOST 漏洞对其企业的影响，有效地追踪这一严重漏洞的修复过程。

参考文献

Qualys Advisory:

<https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt>

RedHat: <https://rhn.redhat.com/errata/RHSA-2015-0090.html>

Ubuntu: <https://launchpad.net/ubuntu/+source/eglibc>

Debian: <https://security-tracker.debian.org/tracker/CVE-2015-0235>

GNU C Library: <http://www.gnu.org/software/libc/>

Mitre: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235>