预警编号：YJ-2017028

恒安嘉新

关于 GNU Wget 存在缓冲区溢出漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 11 月 13 日

1 漏洞描述

近期，互联网爆出两个缓冲区溢出漏洞（CVE-2017-13089、CVE-2017-13090），使用存在漏洞的 Wget 可能受到恶意 HTTP 响应攻击，导致拒绝服务和恶意代码执行。漏洞的详细细节和利用代码已公开，近期被不法分子利用出现大规模攻击尝试的可能性较大。漏洞危害程度为高危(High)。

2 影响范围

漏洞影响 1.19.2 之前版本。

由于 Wget 是 Unix/linux 发行版的基本组件，因此几乎所有发行版或封装调用 Wget 的应用都受影响，包括一些主流的 Linux 发行版：Red Hat、Debian、Ubuntu、SUSE、Gentoo、CentOS、FreeBSD、Oracle Linux、Amazon Linux AMI 等默认带有 Wget 的 Linux 发行版众多。

请参考各发行版受影响范围：

Red Hat Enterprise Linux 7

https://access.redhat.com/security/cve/CVE-2017-13089

https://access.redhat.com/security/cve/CVE-2017-13090

SUSE(SUSE Linux Enterprise Server/openSUSE)

https://www.suse.com/security/cve/CVE-2017-13089/

https://www.suse.com/security/cve/CVE-2017-13090/

Debian

https://security-tracker.debian.org/tracker/CVE-2017-13089

https://security-tracker.debian.org/tracker/CVE-2017-13090

Found in versions Wget/1.16-1, Wget/1.19.1-5

Fixed in versions 1.16-1+deb8u4, 1.18-5+deb9u1, Wget/1.19.2-1

Ubuntu

https://people.canonical.com/~ubuntu-security/cve/2017/CVE-2017-13089.html

https://people.canonical.com/~ubuntu-security/cve/2017/CVE-2017-13090.html

https://usn.ubuntu.com/usn/usn-3464-1/

https://usn.ubuntu.com/usn/usn-3464-2/

Ubuntu 17.10 Wget 1.19.1-3ubuntu1.1

Ubuntu 17.04 Wget 1.18-2ubuntu1.1

Ubuntu 16.04 LTS Wget 1.17.1-1ubuntu1.3

Ubuntu 14.04 LTS Wget 1.15-1ubuntu1.14.04.3

Ubuntu 12.04 LTS Wget 1.13.4-2ubuntu1.5

Gentoo

https://bugs.gentoo.org/show_bug.cgi?id=CVE-2017-13089

https://bugs.gentoo.org/show_bug.cgi?id=CVE-2017-13090

Oracle Linux version 7

https://linux.oracle.com/cve/CVE-2017-13089.html

https://linux.oracle.com/cve/CVE-2017-13090.html

Amazon Linux AMI

https://alas.aws.amazon.com/ALAS-2017-916.html

CentOS

https://lists.centos.org/pipermail/centos-announce/2017-October/022609.html

FreeBSD

https://reviews.freebsd.org/rP453520

3 漏洞原理

2017 年 10 月 26 日，GNU Wget 发布了 1.19.2 之前版本的缓冲区溢出漏洞公告，使用存在漏洞的 Wget 可能受到恶意 HTTP 响应攻击，导致拒绝服务和恶意代码执行，相关漏洞信息如下：

CVE-2017-13089：漏洞在 src/http.c 源码文件中，Wget 在一些调用 http.c:skip_short_body() 函数情况下，块解析器使用 strtol() 读取每个响应分块的长度，但不检查块长度是否为非负数，而在 Wget 调用过程中该数据内容和长度可以完全被攻击者控制，从而导致最终在 fd_read（）函数中触发栈缓冲区溢出。

CVE-2017-13090：漏洞在 src/retr.c 源码文件中，Wget 在一些调用 retr.c:fd_read_body()函数情况下，块解析器使用 strtol() 读取每个响应分块的长度，但不检查块长度是否为非负数，而在 Wget 调用过程中该数据内容和长度可以完全被攻击者控制，从而导致最终在 fd_read( )函数中触发堆缓冲区溢出。

4 修复建议

厂商已在最新发布的 Wget 1.19.2 版本中修复了上述漏洞，强烈建议参照对应发行版的安全更新指南尽快升级到无漏洞版本。汇集各发行版安全公告列表参考：

https://security.archlinux.org/CVE-2017-13089

https://security.archlinux.org/CVE-2017-13090

另，不能及时升级的用户，可采取如下临时解决方案：

Wget 是 Unix/linux 上基本组件，建议使用 Linux 发行版的企业通过安全配置基线统一实施加固措施，如：限制 Wget 访问外部 HTTP。