技術ノート KGTN 2014041502

現 象

[GGFU] OpenSSL の脆弱性（CVE-2014-0160, Heartbeat overflow issue）に関して， GO-Global for Unix についてはどうか？

説 明

2.2.15 またはそれ以前のバージョンについては，影響を受けません．2.2.16 またはそれ以降のバージョンについては，Linux 版以外については影響を受けません．Linux 版については，ディストリビューションに含まれる OpenSSL を使用するため，そのディストリビューションの影響に従います．

GO-Global for UNIX version 2.2.15 and earlier are not vulnerable on all supported platforms. GO-Global for UNIX version 2.2.16 and later are not vulnerable on all non-Linux platforms. On Linux, GO-Global for UNIX version 2.2.16 and later use the operating system's version of OpenSSL. Some supported Linux distributions may be vulnerable.

There are several avenues that would lead to fixing the vulnerability:

- upgrading to OpenSSL 1.0.1g
- downgrading to an OpenSSL 1.0.0 version
- recompiling a vulnerable OpenSSL 1.0.1 version with -DOPENSSL_NO_HEARTBEATS

The only supported Linux platform that we are aware of that is vulnerable to this bug is Red Hat Enterprise LInux 6.5. They have released new openssl packages that are based on OpenSSL 1.0.1e compiled with -DOPENSSL_NO_HEARTBEATS:

https://rhn.redhat.com/errata/RHSA-2014-0376.html

Last reviewed: Apr 16, 2014
Status: DRAFT
Ref: CASE#41254, CVE-2014-0160