GovCERT.HK

Weekly IT Security News Bulletin, 2017-W27

3 July – 9 July 2017

Headlines

Researchers crack GnuPG crypto library to steal 1024-bit RSA encryption private key

- GNU Privacy Guard (GnuPG) is an open source encryption program commonly used in Linux, macOS, Windows and Android. A vulnerability (CVE-2017-7526) was found in its "Libgcrypt" cryptographic library, allowing an attacker to extract the RSA-1024 private key used to decrypt the protected data.

- The "Libgcrypt" library adopts the "left-to-right sliding windows" method to compute the mathematics for data encryption. The method leaks so much information about exponent bits that full RSA key recovery is viable via a side-channel attack.

- The side-channel attack is intended to break a cryptosystem based on analysis of information exposed from the physical implementation of the system, such as timing information, electromagnetic leaks, power consumption, shared cache memory, etc. On a vulnerable virtual system or cloud environment, one virtual machine (VM) could be used to steal private keys from another VM, by launching the side-channel attack. The GnuPG team has released Libgcrypt version 1.7.8 to avoid the exploitation.

Advice

- Update your relevant systems with the latest Libgcrypt version.

- Do not share the same computer platform for critical systems with others, to defend against the side-channel attack from co-resident systems.

Sources

- International Association for Cryptologic Research - Sliding Right into Disaster
- Gnupg.org – Release to fix CVE-2017-7526
- Threatpost

CopyCat malware infected 14 million Android devices around the world

- CopyCat is an adware that generates and steals ad revenues by infecting Android mobile devices. As recorded in one of its Command and Control servers, there were over 14 million devices infected between April and May 2016. Its spreading was reported to be made via repackaged popular apps downloaded from third party app stores and phishing messages. No evidence indicates that it was distributed on Google Play, Google's official app store.

- Once the user has downloaded and installed the CopyCat, it roots the user device to gain the full control. Malicious code will be injected into the Zygote app launching process, which is the parent daemon of all running Android apps. Then it reaps advertisement revenue by displaying fraudulent ads itself and replacing the referrer IDs of other legitimate apps with its own.

- The malware exploits couples of years old Android vulnerabilities (CVE-2013-6282, CVE-2014-3153, CVE-2014-4321, CVE-2014-4324 and CVE-2015-3636), relevant to Android version 5 and earlier, to escalate privileges of the infected current user to root. With the root privilege, it can root the device, inject malicious shared library into system processes, install fraudulent apps silently, steal credit for app installations, and display fraudulent ads. It is also designed with anti-malware and anti-fraud evasion features to undermine the effectiveness of the detective solutions.

Advice

- Update your Android devices with latest security patches and operating system versions available.

- Download and install apps only from official and trustable app stores.

Sources

- Check Point Blog
- CopyCat Research Report

Dumping credentials from Windows Local Security Authority Subsystem (LSASS) for malware spreading

- The widely spread Petrwrap ransomware will install a credential dumping tool on a Windows-based computer after infecting it. The tool was reprogrammed based on an open source project in GitHub named Mimikatz for retrieving Windows system credentials and use them to gain further access of systems in the network. Mimikatz requires the administrator privilege to execute, however.

- Credentials, such as login ids and passwords, in Windows-based systems are stored as a reversibly encrypted plaintext. They will be decrypted by the Local Security Authority Subsystem (LSASS) process using a built-in dynamic-link library (DLL), Wdigest.dll, in order to derive the key for authentication. After the authentication process, the encrypted credentials are stored in the memory for subsequent usage, until the system is rebooted.

- A properly configured Windows system will only allow the operating system to perform the decryption on those credentials in the memory. However, the credential dumping tool, if executed with the administrator right, can run in debug mode to inject a malicious DLL to the LSASS process. The malicious DLL can dump the credentials from the memory and decrypt them in plaintext by abusing the Wdigest.dll.

Advice

- Adopt the principle of least privilege so that end user accounts should be deprived of the administrative privilege.

- Keep the anti-malware program and signatures up-to-date against variants of hacking tools.

Sources

- Microsoft: Cached and Stored Credentials, Digest Authentication
- GitHub - Mimikatz
- Open Security Research
- CrowdStrike

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-July/022492.html
   https://lists.centos.org/pipermail/centos-announce/2017-July/022493.html
   https://lists.centos.org/pipermail/centos-announce/2017-July/022494.html

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-FireSIGHT
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-asrcmd
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-cpn
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-esc1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-esc2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-ios
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-iosxr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-ise1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-ise2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-prime
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-staros
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-uas
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-waas
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-waas1

3. **Debian**
   https://www.debian.org/security/2017/dsa-3901
   https://www.debian.org/security/2017/dsa-3902
   https://www.debian.org/security/2017/dsa-3903

4. **F5 Products**
   https://support.f5.com/csp/article/K02230327
   https://support.f5.com/csp/article/K37830055
   https://support.f5.com/csp/article/K42903299
   https://support.f5.com/csp/article/K59448931

5. **Gentoo Linux**
   https://security.gentoo.org/glsa/201707-01

6. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170705-01-tls-en

7. **Joomla**
   https://www.joomla.org/announcements/release-news/5709-joomla-3-7-3-release.html
   https://www.hkcert.org/my_url/en/alert/17070601

8. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0199.html
   http://advisories.mageia.org/MGASA-2017-0200.html

9. **openSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00006.html
   https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00007.html

10. **Oracle Linux**
   https://linux.oracle.com/errata/ELSA-2017-1479.html
   https://linux.oracle.com/errata/ELSA-2017-1482-1.html
   https://linux.oracle.com/errata/ELSA-2017-1679.html
   https://linux.oracle.com/errata/ELSA-2017-1680.html
   https://linux.oracle.com/errata/ELSA-2017-1681.html
   https://linux.oracle.com/errata/ELSA-2017-3589.html
   https://linux.oracle.com/errata/ELSA-2017-3590.html
   https://linux.oracle.com/errata/ELSA-2017-3591.html

11. **Red Hat**
   https://access.redhat.com/errata/RHSA-2017:1677
   https://access.redhat.com/errata/RHSA-2017:1678
   https://access.redhat.com/errata/RHSA-2017:1679
   https://access.redhat.com/errata/RHSA-2017:1680
   https://access.redhat.com/errata/RHSA-2017:1681
   https://access.redhat.com/errata/RHSA-2017:1682
   https://access.redhat.com/errata/RHSA-2017:1685
   https://access.redhat.com/errata/RHSA-2017:1712

12. **Slackware**
   http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.564513
   http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.614045
   http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.852574

13. **Schneider Electric Wonderware ArchestrA Logger**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-187-04

14. **Siemens**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-187-01
   https://ics-cert.us-cert.gov/advisories/ICSA-17-187-02
   https://ics-cert.us-cert.gov/advisories/ICSA-17-187-03

15. **SUSE**
   https://www.suse.com/support/update/announcement/2017/suse-su-20171741-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171742-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171743-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171744-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171745-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171760-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171763-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171769-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171770-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171771-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171773-1.html
   https://www.suse.com/support/update/announcement/2017/suse-su-20171774-1.html

https://www.suse.com/support/update/announcement/2017/suse-su-20171775-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171777-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171778-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171783-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171790-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171792-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171793-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171794-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171795-1.html

16. Ubuntu

https://www.ubuntu.com/usn/usn-3347-1/
https://www.ubuntu.com/usn/usn-3348-1/
https://www.ubuntu.com/usn/usn-3349-1/

Sources of product vulnerability information:

CentOS
Cisco
Debian
F5
Gentoo Linux
HKCERT
Huawei
ICS-CERT
Joomla
Mageia
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu

Contacts:

cert@govcert.gov.hk