GovCERT.HK

Weekly IT Security News Bulletin, 2017-W45

6 November – 12 November 2017

Headlines

Misconfigured cloud storages vulnerable to GhostWriter attack

- A new type of attack, dubbed "GhostWriter", targets misconfigured Amazon Simple Storage Service (S3) buckets was identified. The GhostWriter attackers scan the Internet to look for misconfigured S3 buckets left exposed online for write access. They then replace the legitimate files with malicious ones. JavaScript or other code storing in the vulnerable buckets could be silently overwritten for drive-by attacks, bit-coin mining or other exploits for steganography attacks or malware distribution.

- A cloud security company Skyhigh scanned over 1,600 S3 buckets and identified about 4% were misconfigured and vulnerable to GhostWriter. The same company has also released in September 2017 the statistics indicating that 7% of all S3 buckets got unrestricted public read access and 35% are unencrypted, allowing anyone to view their content.

- Amazon S3 is a cloud-based service, which provides a web services interface for web applications to store and retrieve data over the Internet. Under normal circumstances, Amazon users create and configure containers called buckets at the service cloud for storing their data objects, such as photos, videos, documents, programs, etc. and delivering these contents through web sites and applications. Hence, both owners of data residing in S3 and enterprises accessing this content from their internal networks are required to take necessary actions to protect themselves from malicious Man-in-the-Middle attacks.

Advice

- Understand the cloud service's access policy options and configure who has read and/or write access on need basis.

- Deploy encryption and digital signatures for data objects stored in the cloud to protect their confidentiality and integrity.

- Monitor for suspicious activities such as unauthorised access or modification to data objects stored in the cloud.

Sources

- AWS
- Bleeping Computer
- Skyhigh

Banking Trojan targets search results

- Google has been commonly used by Internet users to find information, but the links returned are not necessarily safe. A whole attack framework was disclosed abusing search engine optimization (SEO) techniques to "poison" the Search Engine Results Page (SERP) for distributing the Zeus Panda banking Trojan to target victims.

- When specific sets of financial-related search keywords were used by the target victims, the attackers succeeded in ensuring that links to their compromised websites would be ranked highly by the search engines, thus increasing the chance of getting their poisoned results clicked by the victims. Once the victims browsed the compromised websites, a multi-stage malware infection process would be triggered.

- On the other hand, Google's Safe Browsing service identifies unsafe websites across the web by examining their URLs, software and content. If a harmful website is detected, users will be notified with a warning next to that site on the SERP. A Safe Browsing-enabled browser will also display a warning web page if users are trying to access the harmful website.

Advice

- Be mindful that links in search results are not guaranteed to be safe.

- Enable safe-browsing features of your browser whatever available, such as pop-up blockers, ad blockers, antispyware, antivirus, anti-phishing, and private modes.

- Keep your browser and operating system update with the latest versions or security patches.

Sources

- Cisco Talos
- Sucuri
- Google

Product Vulnerability Notes & Security Updates

1. **Apple iOS**
   https://support.apple.com/kb/HT208255

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-November/022612.html

3. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171103-bgp

4. **Debian**
   https://www.debian.org/security/2017/dsa-4016
   https://www.debian.org/security/2017/dsa-4017
   https://www.debian.org/security/2017/dsa-4018
   https://www.debian.org/security/2017/dsa-4019
   https://www.debian.org/security/2017/dsa-4020
   https://www.debian.org/security/2017/dsa-4021
   https://www.debian.org/security/2017/dsa-4022
   https://www.debian.org/security/2017/dsa-4023
   https://www.debian.org/security/2017/dsa-4024
   https://www.debian.org/security/2017/dsa-4025
   https://www.debian.org/security/2017/dsa-4026
   https://www.debian.org/security/2017/dsa-4027
   https://www.debian.org/security/2017/dsa-4028
   https://www.debian.org/security/2017/dsa-4029
   https://www.debian.org/security/2017/dsa-4030

5. **F5 Products**
   https://support.f5.com/csp/article/K33567812
   https://support.f5.com/csp/article/K42185012
   https://support.f5.com/csp/article/K65615624
   https://support.f5.com/csp/article/K75543432

6. **Fortinet FortiOS**
   https://fortiguard.com/psirt/FG-IR-17-137
   https://fortiguard.com/psirt/FG-IR-17-168

7. **Google Chrome**
   https://chromereleases.googleblog.com/2017/11/stable-channel-update-for-desktop.html

8. **Gentoo Linux**
   https://security.gentoo.org/glsa/201711-01

9. **IBM InfoSphere Guardium Data Redaction**
   http://www-01.ibm.com/support/docview.wss?uid=swg22008888

10. **Joomla!**
    https://www.joomla.org/announcements/release-news/5716-joomla-3-8-2-release.html
    https://www.hkcert.org/my_url/en/alert/17110802

11. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0401.html
    http://advisories.mageia.org/MGASA-2017-0402.html
    http://advisories.mageia.org/MGASA-2017-0403.html
    http://advisories.mageia.org/MGASA-2017-0404.html
    http://advisories.mageia.org/MGASA-2017-0405.html

12. **OpenSSL**
    https://www.openssl.org/news/secadv/20171102.txt

13. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00007.html
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00008.html
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00009.html
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00012.html

14. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:3123
    https://access.redhat.com/errata/RHSA-2017:3124
    https://access.redhat.com/errata/RHSA-2017:3141
    https://access.redhat.com/errata/RHSA-2017:3151

15. **Schneider Electric InduSoft Web Studio**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-313-02

16. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.393003
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.493670

17. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20172931-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172932-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172933-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172935-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172936-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172937-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172946-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172947-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172948-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172949-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172950-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172951-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172952-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172956-1/

18. **Symantec Endpoint Protection**
    https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20171106_00

19. **Ubuntu**
    https://usn.ubuntu.com/usn/usn-3346-3/

https://usn.ubuntu.com/usn/usn-3473-1/
https://usn.ubuntu.com/usn/usn-3474-1/
https://usn.ubuntu.com/usn/usn-3475-1/
https://usn.ubuntu.com/usn/usn-3476-1/

Sources of product vulnerability information:

Apple
CentOS
Cisco
Debian
F5
Fortinet
Gentoo Linux
Google Chrome
HKCERT
IBM
ICS-CERT
Joomla!
Mageia
OpenSSL
openSUSE
Red Hat
Slackware
SUSE
Symantec
Ubuntu

Contacts:

cert@govcert.gov.hk