GovCERT.HK

Weekly IT Security News Bulletin, 2017-W44

30 October – 5 November 2017

Headlines

Estonia freezes 760,000 vulnerable resident ID cards

- The Estonia government announced that all of the country's digital ID cards issued between 16 October 2014 and 25 October 2017 were vulnerable to identify theft and would be suspended until the card holders have updated their certificates with the fix. 760,000 individuals, which accounted for half of the country's population, were affected.

- The vulnerability was discovered in software installed on the embedded chip used in the ID cards, resulting in weaker public keys subject to be compromised. The ID cards were manufactured by the Swiss company Trub AG and its successor Gemalto AG, which were helping the Estonian government to solve the problem in September 2017. The ID program's managing director asserted that there have been no reported incidents of any ID or ID card being misused via the vulnerability and the attack demanded considerable resources and expertise.

- Since 31 October 2017, all holders of the faulty ID cards could update their certificates remotely using the Estonian ID card utility software, which may take up to 15 minutes to complete, or at Estonian police and border guard service points. The deadline for the update is 31 March 2018 after which the unpatched card holder would have to apply for a new card.

Advice

- Other cards based on the same faulty chips are exposed to the same cyber risk, so card system owners should check whether they are using the vulnerable chips.

- The affected systems should be patched and the previously generated cryptographic keys should be revoked and re-generated.

- System developers should ensure that security management is included in the system design such that patches could be deployed effectively and timely to minimise impacts to users.

Sources

- Estonia E-Residency Blog
- Security Affairs
- Postimees

Abuse of RDP for Crysis ransomware implantation

- Remote Desktop Protocol (RDP) is a proprietary protocol running on all Microsoft Windows systems. It allows a user to log in a remote computer and control its operations over the network, as on a local computer.

- Security researchers in the industry noticed an increase in reports of malicious activities using the RDP worldwide. The Crysis ransomware family is one of them and has caused waves of attacks since it was first identified in 2016. Locally, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) also received a number of infection reports of Crysis ransomware in October 2017.

- Without the use of phishing emails or compromised websites for propagation, Crysis ransomware compromises computers through their exposed RDP port (TCP 3389) and commonly used credentials without any user interactions. The ransomware encrypts files on infected computers, as well as any connected network drives. The encrypted files are appended with ".arena" at the end of their filename extensions.

Advice

- Block RDP protocol access from the Internet unless additional protective measures, such as virtual private network (VPN) and multiple-factor authentication, are implemented.

- Disable access to shared drives and the clipboard by the Remote Desktop Services for limiting the ability to copy files via RDP.

- Keep anti-malware software and signatures up-to-date on all computer systems.

- Perform regular backups on important data assets and keep the backup copies disconnected from the computer.

Sources

- Trend Micro
- HKCERT

Combosquatting: a simple trick but a growing threat

- Combosquatting is an attack strategy in which adversaries register domains that combine popular trademarked names with other words designed to trick Internet users into believing the malicious domains are legitimate; for example, yahoofiles[.]com, googlegl[.]com, facebookbchsscience[.]com, etc. Unlike typosquatting, which makes up domains from incorrectly typed trademarked names, combosquatting must contain the trademarks intact.

- At the 2017 ACM Conference on Computer and Communications Security, researchers from the Georgia Institute of Technology and Stony Brook University presented their large-scale empirical study of combosquatting. By analyzing more than 468 billion domain name look-up requests in a six-year data set, the researchers discovered 2.7 million combosquatting domains for 268 popular trademarks, with 60% of the domains kept operating for almost three years. The number of combosquatting domains registered also increased year on year between 2011 and 2016.

- Combosquatting domains are used to provide malicious links embedded in emails, web advertising or the results of web searches, facilitating attacks including phishing, social engineering, affiliate abuse, trademark abuse, and even advanced persistent threats. The abusive domains with a familiar trademark could even give a false sense of comfort to security people who are monitoring network traffic for malicious activity.

Advice

- Users should double-check URLs before clicking on them and avoid clicking on even familiar URLs in unsolicited emails.

- Network administrators should block the known malicious domains, URLs and IP addresses at the network level.

- Domain owners should monitor for malicious registrations involving their domain names and inform users and the public timely to prevent the attacks.

Sources

- Georgia Tech Research Horizons
- Georgia Tech Institute for Information Security & Privacy (Presentation Slides)
- Cornell University Library (Research Paper)

Product Vulnerability Notes & Security Updates

1. **Advantech WebAccess**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-306-02

2. **Apache OpenOffice**
   http://www.openoffice.org/security/cves/CVE-2017-3157.html
   http://www.openoffice.org/security/cves/CVE-2017-9806.html
   http://www.openoffice.org/security/cves/CVE-2017-12607.html
   http://www.openoffice.org/security/cves/CVE-2017-12608.html

3. **Apple iOS, MacOS, iTunes for Windows, Safari and iCloud**
   https://support.apple.com/kb/HT208221
   https://support.apple.com/kb/HT208222
   https://support.apple.com/kb/HT208223
   https://support.apple.com/kb/HT208224
   https://support.apple.com/kb/HT208225

4. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-October/022608.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022609.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022610.html
   https://lists.centos.org/pipermail/centos-announce/2017-October/022611.html

5. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-apicem
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-arce
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-cpcp
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-fpwr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-iosap
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-ise
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-webex1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-webex2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc4

6. **Debian**
   https://www.debian.org/security/2017/dsa-4007
   https://www.debian.org/security/2017/dsa-4008
   https://www.debian.org/security/2017/dsa-4009
   https://www.debian.org/security/2017/dsa-4010
   https://www.debian.org/security/2017/dsa-4011

https://www.debian.org/security/2017/dsa-4012
https://www.debian.org/security/2017/dsa-4013
https://www.debian.org/security/2017/dsa-4015

7. **F5 Products**
   https://support.f5.com/csp/article/K35104614
   https://support.f5.com/csp/article/K62832776
   https://support.f5.com/csp/article/K74413297

8. **Gentoo Linux**
   https://security.gentoo.org/glsa/201710-28
   https://security.gentoo.org/glsa/201710-29
   https://security.gentoo.org/glsa/201710-30
   https://security.gentoo.org/glsa/201710-31
   https://security.gentoo.org/glsa/201710-32

9. **IBM Products**
   http://www-01.ibm.com/support/docview.wss?uid=swg22007462
   http://www-01.ibm.com/support/docview.wss?uid=swg22009950
   http://www-01.ibm.com/support/docview.wss?uid=swg22009996
   http://www-01.ibm.com/support/docview.wss?uid=swg22010172

10. **Juniper Junos OS**
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10818

11. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0389.html
    http://advisories.mageia.org/MGASA-2017-0390.html
    http://advisories.mageia.org/MGASA-2017-0391.html
    http://advisories.mageia.org/MGASA-2017-0392.html
    http://advisories.mageia.org/MGASA-2017-0393.html
    http://advisories.mageia.org/MGASA-2017-0394.html
    http://advisories.mageia.org/MGASA-2017-0395.html
    http://advisories.mageia.org/MGASA-2017-0396.html
    http://advisories.mageia.org/MGASA-2017-0397.html
    http://advisories.mageia.org/MGASA-2017-0398.html
    http://advisories.mageia.org/MGASA-2017-0399.html
    http://advisories.mageia.org/MGASA-2017-0400.html

12. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00076.html
    https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00081.html
    https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00082.html
    https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00083.html
    https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00084.html
    https://lists.opensuse.org/opensuse-security-announce/2017-10/msg00085.html
    https://lists.opensuse.org/opensuse-security-announce/2017-11/msg00000.html

13. **Oracle Identity Manager**
    http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-10151-4016513.html

14. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-3080.html

https://linux.oracle.com/errata/ELSA-2017-3081.html
https://linux.oracle.com/errata/ELSA-2017-3111.html
https://linux.oracle.com/errata/ELSA-2017-3635.html
https://linux.oracle.com/errata/ELSA-2017-3636.html
https://linux.oracle.com/errata/ELSA-2017-3637.html

15. **PHP**
    http://www.php.net/ChangeLog-5.php#5.6.32

16. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:3080
    https://access.redhat.com/errata/RHSA-2017:3081
    https://access.redhat.com/errata/RHSA-2017:3082
    https://access.redhat.com/errata/RHSA-2017:3086
    https://access.redhat.com/errata/RHSA-2017:3093
    https://access.redhat.com/errata/RHSA-2017:3107
    https://access.redhat.com/errata/RHSA-2017:3108
    https://access.redhat.com/errata/RHSA-2017:3110
    https://access.redhat.com/errata/RHSA-2017:3111
    https://access.redhat.com/errata/RHSA-2017:3113
    https://access.redhat.com/errata/RHSA-2017:3114
    https://access.redhat.com/errata/RHSA-2017:3115

17. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.428808
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.534644

18. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20172864-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172869-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172871-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172872-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172873-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172907-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172908-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172920-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172921-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172922-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172923-1/
    https://www.suse.com/support/update/announcement/2017/suse-su-20172924-1/

19. **Trihedral Engineering Limited VTScada**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-304-02

20. **Ubuntu**
    https://usn.ubuntu.com/usn/usn-3426-2/
    https://usn.ubuntu.com/usn/usn-3459-2/
    https://usn.ubuntu.com/usn/usn-3464-2/
    https://usn.ubuntu.com/usn/usn-3467-1/
    https://usn.ubuntu.com/usn/usn-3468-1/
    https://usn.ubuntu.com/usn/usn-3468-2/

https://usn.ubuntu.com/usn/usn-3468-3/
https://usn.ubuntu.com/usn/usn-3469-1/
https://usn.ubuntu.com/usn/usn-3469-2/
https://usn.ubuntu.com/usn/usn-3470-1/
https://usn.ubuntu.com/usn/usn-3470-2/
https://usn.ubuntu.com/usn/usn-3471-1/
https://usn.ubuntu.com/usn/usn-3472-1/

21. **WordPress**
https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/

Sources of product vulnerability information:

Apple
CentOS
Cisco
Debian
F5
Gentoo Linux
IBM
ICS-CERT
Juniper
Mageia
OpenOffice
openSUSE
Oracle
Oracle Linux
PHP
Red Hat
Slackware
SUSE
Ubuntu
WordPress

Contacts:

cert@govcert.gov.hk