GovCERT.HK

Weekly IT Security News Bulletin, 2020-W37

7 September – 13 September 2020

Headlines

Malicious Excel files bypass security screening

- A trick was discovered by cyber criminals to generate malicious Excel files that could be more likely to escape from being caught by security scanners. A threat group called Epic Manchego was reported to have been launching global phishing attacks using emails containing such malicious Excel files since June 2020.

- The trick is to generate the Excel file with a .NET library named EPPlus instead of creating it from the standard Microsoft Office software. The EPPlus library provides the "Export as Excel" and "Save as spreadsheet" functions for compiling Excel files in various formats. The Epic Manchego utilised the functions to create spreadsheets in the Office Open XML (OOXML) format.

- Unlike Excel files saved by the Microsoft Office software, the OOXML files generated via the EEPlus library functions are deprived of a section of complied Visual Basic Application (VBA) code, which would be inspected by some antivirus and email scanners to check if malicious code is stored there. Without the section, the attacker could still hide its malicious code in another password-protected custom VBA code format so as to evade detections while the malicious code still works as a macro script once the user opens the Excel file.

Advice

- Educate end users not to open attachments of unsolicited emails.

- Disable macro running by default on the Microsoft Office Software.

- Keep anti-malware software and other security systems up-to-date to cope with evolving attack methods.

Sources

- NVISO
- ZDNet

A survey on identity security

- The Identity Defined Security Alliance (IDSA) is an industrial association that provides vendor-neutral guidance and resources to organisations for preventing identity-related breaches. It recently conducted an online survey of around 500 IT security and identity security professionals in the United States and came up with trends in identity-related security and how the "forward-thinking" security culture of organisations made a difference in mitigating risks of breaches.

- The trends indicated that identity-related breaches were pervasive. About 94% of respondents have encountered such breaches and 79% of them happened within recent two years. Two-thirds of the organisations regarded phishing as the most common cause of the breaches while 99% believed that the breaches could in fact be prevented.

- For preventive actions, around half of the organisations granted privileged access rights based on the principle of least privilege. Newer effective measures against phishing attempts including using device characteristics or expected user behaviour for authentication were also adopted by some forward-thinking organisations which proactively predicted future identity risks and planned for advanced mitigation measures. The survey found that organisations with the forward-thinking security culture were 25% less likely to get an identity-related breach than organisations with a reactive security culture.

Advice

- Adopt stringent privileged access management based on the principle of least privilege for system and data access, and review your privileged access rights granted on a regular basis.

- Train employees to defend phishing attacks, especially those that could steal their identities and credentials.

- Identify potential identity security threats and keep abreast with latest security technologies for forward-planning mitigation measures against forthcoming risks.

Sources

- Forbes
- GlobeNewswire

Product Vulnerability Notes & Security Updates

1. **Android**

   https://source.android.com/security/bulletin/2020-09-01

2. **AVEVA Enterprise Data Management Web**

   https://us-cert.cisa.gov/ics/advisories/icsa-20-254-01

3. **Citrix StoreFront**

   https://support.citrix.com/article/CTX277455

4. **Debian**

   https://www.debian.org/security/2020/dsa-4758
   https://www.debian.org/security/2020/dsa-4759
   https://www.debian.org/security/2020/dsa-4760
   https://www.debian.org/security/2020/dsa-4761
   https://www.debian.org/security/2020/dsa-4762

5. **F5 Products**

   https://support.f5.com/csp/article/K35226442
   https://support.f5.com/csp/article/K55376430
   https://support.f5.com/csp/article/K91158923

6. **FATEK Automation PLC WinProladder**

   https://us-cert.cisa.gov/ics/advisories/icsa-20-254-02

7. **Gentoo Linux**

   https://security.gentoo.org/glsa/202009-01
   https://security.gentoo.org/glsa/202009-02
   https://security.gentoo.org/glsa/202009-03

8. **Google Chrome**

   https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop.html

9. **IBM WebSphere Application Server**

   https://www.ibm.com/support/pages/node/6328895

10. **Intel Products**

    https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00347.html
    https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00356.html
    https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00404.html
    https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00405.html

11. McAfee Products

https://kc.mcafee.com/corporate/index?page=content&id=SB10327
https://kc.mcafee.com/corporate/index?page=content&id=SB10328

12. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00010.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00011.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00012.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00013.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00014.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00015.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00016.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00017.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00018.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00019.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00020.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00021.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00022.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00024.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00025.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00027.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00028.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00029.html

13. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-3556.html
https://linux.oracle.com/errata/ELSA-2020-3623.html
https://linux.oracle.com/errata/ELSA-2020-3654.html
https://linux.oracle.com/errata/ELSA-2020-3658.html
https://linux.oracle.com/errata/ELSA-2020-3662.html
https://linux.oracle.com/errata/ELSA-2020-3669.html
https://linux.oracle.com/errata/ELSA-2020-5841.html
https://linux.oracle.com/errata/ELSA-2020-5844.html
https://linux.oracle.com/errata/ELSA-2020-5845.html

14. Red Hat

https://access.redhat.com/errata/RHSA-2020:3578
https://access.redhat.com/errata/RHSA-2020:3616
https://access.redhat.com/errata/RHSA-2020:3625
https://access.redhat.com/errata/RHSA-2020:3637
https://access.redhat.com/errata/RHSA-2020:3638
https://access.redhat.com/errata/RHSA-2020:3639
https://access.redhat.com/errata/RHSA-2020:3642
https://access.redhat.com/errata/RHSA-2020:3644
https://access.redhat.com/errata/RHSA-2020:3654
https://access.redhat.com/errata/RHSA-2020:3662
https://access.redhat.com/errata/RHSA-2020:3665
https://access.redhat.com/errata/RHSA-2020:3669
https://access.redhat.com/errata/RHSA-2020:3675
https://access.redhat.com/errata/RHSA-2020:3678
https://access.redhat.com/errata/RHSA-2020:3697
https://access.redhat.com/errata/RHSA-2020:3699
https://access.redhat.com/errata/RHSA-2020:3702
https://access.redhat.com/errata/RHSA-2020:3704
https://access.redhat.com/errata/RHSA-2020:3706
https://access.redhat.com/errata/RHSA-2020:3708
https://access.redhat.com/errata/RHSA-2020:3711
https://access.redhat.com/errata/RHSA-2020:3713
https://access.redhat.com/errata/RHSA-2020:3714
https://access.redhat.com/errata/RHSA-2020:3723

15. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-06
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-05
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-01
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-03
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-08

16. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.337537

17. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20202487-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202491-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202492-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202497-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202498-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202499-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202502-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202505-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202506-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202507-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202508-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202509-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202513-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202515-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202517-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202524-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202525-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202526-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202531-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202534-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202537-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202540-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202541-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202544-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202562-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202563-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202569-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202570-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202574-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202575-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202576-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202577-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202578-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202579-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202580-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202581-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202582-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202583-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202598-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202599-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202600-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202601-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202602-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202603-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202604-1/

18. Trend Micro Products

https://success.trendmicro.com/solution/000267260

19. Ubuntu

https://ubuntu.com/security/notices/USN-4487-2
https://ubuntu.com/security/notices/USN-4488-2
https://ubuntu.com/security/notices/USN-4489-1
https://ubuntu.com/security/notices/USN-4490-1
https://ubuntu.com/security/notices/USN-4491-1

20. Wibu-Systems CodeMeter

https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

Sources of product vulnerability information:

Android
Citrix
Debian
F5
Gentoo Linux
Google Chrome
IBM
Intel
McAfee
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk