GovCERT.HK

Weekly IT Security News Bulletin, 2021-W06

8 February – 14 February 2021

Headlines

Moving towards quantum-proof cryptography

- On 9 February 2021, ENISA published a report to provide latest update on development of post-quantum cryptography (PQC).
- With the advance of the quantum technology, the commonly used encryption algorithms relying on complexity in computation of integer factorisation, discrete logarithm or elliptic-curve discrete logarithm can become insecure when confronted with quantum machines. It becomes important to develop post-quantum cryptographic algorithms to safeguard data against quantum capable hackers.
- The report gives an overview of the latest progress of standardisation process of PQC and highlights five different families of PQC algorithms under research as well as the three finalist proposals for the NIST PQC Standardization Process.
- As the standardisation process can take years to complete, ENISA recommend users who need to preserve the confidentiality of their data for more than a decade to mitigate the risks by adopting a hybrid scheme (i.e., combination of pre-quantum and post quantum solutions) or protective measures (i.e., mix pre-shared keys into all keys created via public-key cryptography).

Advice

- Consider adopting post-quantum algorithms on top of any pre-quantum algorithms wherever possible to provide an additional layer of security on data.
- Regularly review the security of cryptographic schemes in use and adopt solutions which are secure against attacks.

Sources

- ENISA
- NIST

Cyber attack can be life-threatening

- Cyber security is of paramount importance to critical infrastructure and any unauthorised access or manipulation to those industrial control systems can result in grievous harms. An attack of such kind happened in the United States where an attacker successfully broke into the computer system of a water treatment facility and caused malicious mischief by raising the amount of sodium hydroxide applied to drinking water for adjusting water acidity level to a dangerous level.

- To launch the attack, the attacker gained access to a remote desktop software called TeamViewer on a staff's computer via which to gain control of the critical system for a couple of minutes. The concerned user who was monitoring the computer immediately noticed the unauthorised access and reverted the sodium hydroxide level to normal.

- In fact, the water treatment facility, similar to other industrial control systems, has multiple controls in place to detect and prevent any anomaly in in the system settings and processes. Any abnormal sodium hydroxide level detected will trigger alarms so that operators can intervene immediately.

Advice

- Restrict or forbid the use of remote access software on critical systems or computers with special privileges.
- Incorporate monitoring and safety functions into critical system settings and processes to prevent abnormal modification due to human errors or manipulation by malicious actors.

Sources

- Bleeping Computer
- Dark Reading

Product Vulnerability Notes & Security Updates

1. **Advantech iView**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-040-02

2. **Apple macOS**

   https://support.apple.com/en-us/HT212177

3. **CentOS**

   https://lists.centos.org/pipermail/centos-announce/2021-February/048272.html

4. **Debian**

   https://www.debian.org/security/2021/dsa-4846
   https://www.debian.org/security/2021/dsa-4847
   https://www.debian.org/security/2021/dsa-4848
   https://www.debian.org/security/2021/dsa-4849
   https://www.debian.org/security/2021/dsa-4850

5. **F5 Products**

   https://support.f5.com/csp/article/K09121542
   https://support.f5.com/csp/article/K13323323
   https://support.f5.com/csp/article/K29282483
   https://support.f5.com/csp/article/K32049501
   https://support.f5.com/csp/article/K62532228
   https://support.f5.com/csp/article/K63497634
   https://support.f5.com/csp/article/K68652018
   https://support.f5.com/csp/article/K72708443
   https://support.f5.com/csp/article/K76518456
   https://support.f5.com/csp/article/K87502622
   https://support.f5.com/csp/article/K88162221
   https://support.f5.com/csp/article/K88230177

6. **Horner Automation Cscape**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-035-02

7. **Huawei Products**

   https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en
   https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-02-dos-en

8. **IBM WebSphere Application Server**

   https://www.ibm.com/support/pages/node/6413709

9. Intel Products

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00318.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00397.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00425.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00434.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00436.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00438.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00443.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00444.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00445.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00448.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00450.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00451.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00453.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00455.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00456.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00457.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00462.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00471.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00475.html

10. Luxion KeyShot

https://us-cert.cisa.gov/ics/advisories/icsa-21-035-01

11. McAfee Products

https://kc.mcafee.com/corporate/index?page=content&id=SB10345

12. Microsoft Edge (Chromium-based)

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#february-4-2021
https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#february-5-2021

13. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-9028.html
https://linux.oracle.com/errata/ELSA-2021-9029.html
https://linux.oracle.com/errata/ELSA-2021-9034.html
https://linux.oracle.com/errata/ELSA-2021-9035.html
https://linux.oracle.com/errata/ELSA-2021-9037.html
https://linux.oracle.com/errata/ELSA-2021-9038.html
https://linux.oracle.com/errata/ELSA-2021-9039.html
https://linux.oracle.com/errata/ELSA-2021-9040.html
https://linux.oracle.com/errata/ELSA-2021-9041.html
https://linux.oracle.com/errata/ELSA-2021-9043.html

14. Red Hat

https://access.redhat.com/errata/RHSA-2021:0295
https://access.redhat.com/errata/RHSA-2021:0308
https://access.redhat.com/errata/RHSA-2021:0310
https://access.redhat.com/errata/RHSA-2021:0313
https://access.redhat.com/errata/RHSA-2021:0433
https://access.redhat.com/errata/RHSA-2021:0459
https://access.redhat.com/errata/RHSA-2021:0470
https://access.redhat.com/errata/RHSA-2021:0471
https://access.redhat.com/errata/RHSA-2021:0472
https://access.redhat.com/errata/RHSA-2021:0473
https://access.redhat.com/errata/RHSA-2021:0474
https://access.redhat.com/errata/RHSA-2021:0476

15. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-040-03
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-04
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-05
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-06
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-10

16. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.585069

17. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210315-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210316-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210323-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210335-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210341-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210342-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210344-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210347-1
https://www.suse.com/support/update/announcement/2021/suse-su-20210348-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210352-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210353-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210354-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210355-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210359-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210362-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210367-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210377-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210386-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210424-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210425-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210427-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210428-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210430-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20210431-1/

18. Ubuntu

https://ubuntu.com/security/notices/USN-4711-1
https://ubuntu.com/security/notices/USN-4713-2
https://ubuntu.com/security/notices/USN-4717-2
https://ubuntu.com/security/notices/USN-4723-1
https://ubuntu.com/security/notices/USN-4724-1
https://ubuntu.com/security/notices/USN-4725-1
https://ubuntu.com/security/notices/USN-4726-1
https://ubuntu.com/security/notices/USN-4727-1
https://ubuntu.com/security/notices/USN-4728-1
https://ubuntu.com/security/notices/USN-4729-1
https://ubuntu.com/security/notices/USN-4730-1
https://ubuntu.com/security/notices/USN-4731-1

19. VMware

https://www.vmware.com/security/advisories/VMSA-2020-0029.html

Sources of product vulnerability information:

Apple
CentOS
Debian
F5
Huawei
IBM
Intel
McAfee
Microsoft
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
VMware

Contact:

cert@govcert.gov.hk