GovCERT.HK

Weekly IT Security News Bulletin, 2021-W17

26 April – 2 May 2021

Headlines

Secure NFC communication

- Near-field communication (NFC) is a short-range wireless technology which enables NFC-capable devices like smartphones to transfer data to each other and is widely used in various applications like contactless payment and file sharing.

- While the proximity of the communication can provide certain degree of security by only allowing devices close to each other to communicate, the NFC Forum recently released two new specifications, namely NFC Authentication Protocol 1.0 Specification (NAP 1.0) and Logical Link Control Protocol Technical Specification 1.4 (LLCP 1.4), to enhance the security of NFC by setting out a cryptographic framework for data transfer through NFC.

- The NAP 1.0 provides a cryptographic mechanism to establish a secure channel for applications requiring authentication and secured data transfer to avoid eavesdropping. It enables fast authentication and setup of secure communication channel among paired NFC devices with common secret key. The LLCP 1.4 further rides on the NAP 1.0 to set out the processes for communication between two devices.

- Such improvement is considered vital to security of NFC applications by protecting confidentiality and privacy of NFC communications which may involve personal data or sensitive messages. Rather than relying on proprietary implementation, the technical specifications provide a standardised framework for encrypting data transferred via NFC and simplifies the development of secure NFC applications.

Advice

- Check if proper encryption mechanism is adopted in NFC applications and ensure data in transit is properly encrypted to protect against eavesdropping.
- Switch off NFC and applications with NFC function when not in use.

Sources

- NFC Forum
- Help Net Security

Defense against software supply chain attacks

- Software supply chain attack is an emerging threat which targets the software vendor's environment by injecting malicious code to the software for creating vulnerabilities so as to compromise their customers' data and systems. All customers of the software can be compromised by installing the infected software, updates or hotfixes.

- To mitigate the risks of software supply chain attacks, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute for Standards and Technology (NIST) of the United States published a document on defending against software supply chain attacks, aiming to give an overview of associated risks and recommendations.

- It emphasises that organisations should adopt proper risk management program to assess the risks associated with the products and services deployed in their environments and manage the risks through a series of technical and non-technical activities. The Cyber Supply Chain Risk Management framework and the Secure Software Development Framework proposed by NIST are suggested for risk identification, assessment and mitigation. To reduce the risk of malicious software, it is important to establish security requirements and controls for suppliers and ensure secure software development practices are adopted. Vulnerability management program should also be in place in organisations for identifying and mitigating discovered vulnerabilities.

Advice

- Maintain an up-to-date inventory of software, closely collaborate with the suppliers and swiftly respond to any discovered vulnerabilities in the software.
- Adopt risk-based approach when selecting software and regularly review and monitor vendors' capability in vulnerability discovery and patch management.
- Formulate a resilience plan with failover processes and workarounds for key software and identify alternative suppliers.

Sources

- CISA
- Security Week

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/en-us/HT212318
https://support.apple.com/en-us/HT212320
https://support.apple.com/en-us/HT212321
https://support.apple.com/en-us/HT212325
https://support.apple.com/en-us/HT212326
https://support.apple.com/en-us/HT212327

2. Debian

https://www.debian.org/security/2021/dsa-4896
https://www.debian.org/security/2021/dsa-4899
https://www.debian.org/security/2021/dsa-4900
https://www.debian.org/security/2021/dsa-4901
https://www.debian.org/security/2021/dsa-4902
https://www.debian.org/security/2021/dsa-4903
https://www.debian.org/security/2021/dsa-4904
https://www.debian.org/security/2021/dsa-4905
https://www.debian.org/security/2021/dsa-4906

3. Fortinet FortiWAN

https://www.fortiguard.com/psirt/FG-IR-21-048

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-dos-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-02-dos-en

5. Microsoft Edge (Chromium Based)

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-29-2021

6. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-1242.html
https://linux.oracle.com/errata/ELSA-2021-1354.html
https://linux.oracle.com/errata/ELSA-2021-1360.html
https://linux.oracle.com/errata/ELSA-2021-1363.html
https://linux.oracle.com/errata/ELSA-2021-1384.html
https://linux.oracle.com/errata/ELSA-2021-1389.html
https://linux.oracle.com/errata/ELSA-2021-1469.html
https://linux.oracle.com/errata/ELSA-2021-9200.html
https://linux.oracle.com/errata/ELSA-2021-9203.html

7. PHP

https://www.php.net/ChangeLog-7.php#7.3.28
https://www.php.net/ChangeLog-8.php#8.0.5

8. Red Hat

https://access.redhat.com/errata/RHSA-2021:1225
https://access.redhat.com/errata/RHSA-2021:1227
https://access.redhat.com/errata/RHSA-2021:1230
https://access.redhat.com/errata/RHSA-2021:1354
https://access.redhat.com/errata/RHSA-2021:1360
https://access.redhat.com/errata/RHSA-2021:1361
https://access.redhat.com/errata/RHSA-2021:1362
https://access.redhat.com/errata/RHSA-2021:1363
https://access.redhat.com/errata/RHSA-2021:1369
https://access.redhat.com/errata/RHSA-2021:1373
https://access.redhat.com/errata/RHSA-2021:1376
https://access.redhat.com/errata/RHSA-2021:1377
https://access.redhat.com/errata/RHSA-2021:1379
https://access.redhat.com/errata/RHSA-2021:1401
https://access.redhat.com/errata/RHSA-2021:1407
https://access.redhat.com/errata/RHSA-2021:1444
https://access.redhat.com/errata/RHSA-2021:1445
https://access.redhat.com/errata/RHSA-2021:1446
https://access.redhat.com/errata/RHSA-2021:1447
https://access.redhat.com/errata/RHSA-2021:1448
https://access.redhat.com/errata/RHSA-2021:1452
https://access.redhat.com/errata/RHSA-2021:1468
https://access.redhat.com/errata/RHSA-2021:1469

9. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.472514

10. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20211307-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211310-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211313-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211314-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211315-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211325-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211341-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211344-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211347-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211365-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211373-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211395-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211396-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211399-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211401-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211408-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211409-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211412-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211429-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20211430-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211431-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211433-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211435-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211438-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211439-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211440-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211442-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211444-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211445-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114706-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114707-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114708-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114709-1/

11. Texas Instruments SimpleLink

https://us-cert.cisa.gov/ics/advisories/icsa-21-119-01

12. Ubuntu

https://ubuntu.com/security/notices/USN-4892-1
https://ubuntu.com/security/notices/USN-4913-2
https://ubuntu.com/security/notices/USN-4922-2
https://ubuntu.com/security/notices/USN-4926-1
https://ubuntu.com/security/notices/USN-4927-1
https://ubuntu.com/security/notices/USN-4928-1
https://ubuntu.com/security/notices/USN-4929-1
https://ubuntu.com/security/notices/USN-4930-1

Sources of product vulnerability information:

Apple
Debian
Fortinet
Huawei
Microsoft Edge
Oracle Linux
PHP
Red Hat
Slackware
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk