GovCERT.HK

Weekly IT Security News Bulletin, 2022-W17

25 April – 1 May 2022

Headlines

Warning of vulnerabilities in Linux networkd-dispatcher

- Security researchers from Microsoft discovered two vulnerabilities in the networkd-dispatcher service for Linux systems. The vulnerabilities (tracked as CVE-2022-29799 and CVE-2022-29800), collectively known as Nimbuspwn, could be chained together to allow local authenticated attackers to execute arbitrary commands with root privileges.

- The networkd-dispatcher is a component used to dispatch network status changes in many Linux distributions and can execute scripts as root in response to the status changes. Upon review of the networkd-dispatcher source code, the researchers identified a directory traversal vulnerability that could be exploited to gain unauthorised access to restricted directories and files. In addition, the researchers discovered a race condition issue that could be abused by attackers to replace legitimate scripts with malicious ones.

- Through exploiting the two vulnerabilities in the networkd-dispatcher service, the attackers were able to execute their payloads with the root privilege and deploy backdoors or ransomware on the affected systems. Microsoft had informed the networkd-dispatcher's maintainer of the issues and the maintainer immediately released the fixes for the vulnerabilities.

Advice

- Apply the latest security update as soon as possible when the update is available.
- Deploy endpoint detection and response (EDR) solutions with the capability of behavioural analysis for effective detection of malicious code running across systems and networks.

Sources

- SecurityWeek
- Microsoft
- Ars Technica

Refusing to pay ransomware demand

- A security firm published an annual ransomware report highlighting an upward trend in ransom payments demanded by attackers based on a survey of 5,600 organisations across different sectors. The report also revealed that two-third of respondents suffered from ransomware attacks in 2021, indicating that ransomware still continued to be one of the common threats.

- In 2021, the average ransom paid by organisations were around US$812,000, which increased nearly fivefold compared with 2020. According to the security firm, almost half (46%) of the victims paid a ransom while only 4% of them were able to restore all of the encrypted data after paying the ransom.

- While some organisations considered paying the ransom to obtain the decryption key as a faster solution to return to normal operations after a ransomware attack, the survey result showed that paying a ransom does not guarantee the recovery of data and may increase the chance of being targeted again. Conducting regular backups of data and implementing proper security hardening would be the better solutions to protect systems against ransomware attacks.

Advice

- Stay vigilant of the latest ransomware threats and derive recovery plans to mitigate ransomware risks.
- Conduct regular backup of data and systems, test the backups routinely and keep offline backups.
- Educate users on ransomware threats through security awareness training.

Sources

- Sophos
- Dark Reading

Product Vulnerability Notes & Security Updates

1. Debian

https://www.debian.org/security/2022/dsa-5124
https://www.debian.org/security/2022/dsa-5125

2. F5 Products

https://support.f5.com/csp/article/K51975973
https://support.f5.com/csp/article/K53648360

3. Hitachi Energy System Data Manager

https://us-cert.cisa.gov/ics/advisories/icsa-22-116-01

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220427-01-e9a493e2-en

5. IBM Products

https://www.ibm.com/support/pages/node/6575535
https://www.ibm.com/support/pages/node/6575539
https://www.ibm.com/support/pages/node/6575541
https://www.ibm.com/support/pages/node/6575543
https://www.ibm.com/support/pages/node/6575545
https://www.ibm.com/support/pages/node/6575551
https://www.ibm.com/support/pages/node/6575559
https://www.ibm.com/support/pages/node/6575567
https://www.ibm.com/support/pages/node/6575577
https://www.ibm.com/support/pages/node/6575589
https://www.ibm.com/support/pages/node/6575599
https://www.ibm.com/support/pages/node/6575611

6. Johnson Controls Metasys

https://us-cert.cisa.gov/ics/advisories/icsa-22-118-01

7. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/2FTD5LDTBCU5ZUYR3FGZ66MQG2JNI4ED/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3CCOVXHDVS7YA5QUUIFXTDYNR5EEIDAO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4PMS2K6P4NJETZQA4LRNOCXXKHTI7ZE5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6F72F4XQADWZ2XEWVPBHNKW46B6FKIXL/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/COAZMKGIFFK6JHHLFRHHTVMQ4HK5XI73/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DCH7WCUVWWLVX6ITJIZWAVCPF7EKZ2D6/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DR7ZSOKFQZ5EIKQHLZ37AMGVPDGDIJ5W/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ESPDBLVWSZSR5FGSXSIJXGNV5FP6I3Z5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FFGYE7EA6IGB2VAFI7DSL2I7IZA2KXCO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/H4M2ANEJKWG5JH6ZBPU35FCN5CXKBGAP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/L42LORYEBVO26VQBBKI66KR7JJD4LX62/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/OXY7DJ3ZRXW5ELKGQV46EF2S2IYSY5P7/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/QMGM2N6RR7GOZR7OP37QJTCTTLTTIWUN/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/URPSCIIV7ZGEE2LEPVY4Z625INVH7XVQ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/UZKD5U7JDRKQQSTHBB3DHEGKKC7A3UQU/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WDTPE3OWW3XCVF6LBCYZ3YYVTQER23IK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WQT22OV7HHVKNPMZMCT3YW4SACMP6NMZ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/XB7C5ORXK2GBCI6U44YZK35SFTMPSGTI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/XMTGPB2XDXKUXI74SIW34IQGUEL7CL27/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YRULXA6FSWST2PIA5WOTTJOZHYDZKKRZ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZCRJLTSE4Q74IY2S3JMWL4FUJNLTPRKC/

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-1487.html
https://linux.oracle.com/errata/ELSA-2022-1491.html
https://linux.oracle.com/errata/ELSA-2022-1537.html
https://linux.oracle.com/errata/ELSA-2022-1546.html
https://linux.oracle.com/errata/ELSA-2022-1550.html
https://linux.oracle.com/errata/ELSA-2022-1556.html
https://linux.oracle.com/errata/ELSA-2022-1565.html
https://linux.oracle.com/errata/ELSA-2022-1566.html
https://linux.oracle.com/errata/ELSA-2022-1642.html
https://linux.oracle.com/errata/ELSA-2022-9313.html
https://linux.oracle.com/errata/ELSA-2022-9314.html

9. Red Hat

https://access.redhat.com/errata/RHSA-2022:1420
https://access.redhat.com/errata/RHSA-2022:1435
https://access.redhat.com/errata/RHSA-2022:1436
https://access.redhat.com/errata/RHSA-2022:1437
https://access.redhat.com/errata/RHSA-2022:1438
https://access.redhat.com/errata/RHSA-2022:1439
https://access.redhat.com/errata/RHSA-2022:1487
https://access.redhat.com/errata/RHSA-2022:1488
https://access.redhat.com/errata/RHSA-2022:1489
https://access.redhat.com/errata/RHSA-2022:1490
https://access.redhat.com/errata/RHSA-2022:1491
https://access.redhat.com/errata/RHSA-2022:1492
https://access.redhat.com/errata/RHSA-2022:1535
https://access.redhat.com/errata/RHSA-2022:1537
https://access.redhat.com/errata/RHSA-2022:1539
https://access.redhat.com/errata/RHSA-2022:1540
https://access.redhat.com/errata/RHSA-2022:1541
https://access.redhat.com/errata/RHSA-2022:1546
https://access.redhat.com/errata/RHSA-2022:1550
https://access.redhat.com/errata/RHSA-2022:1552
https://access.redhat.com/errata/RHSA-2022:1555
https://access.redhat.com/errata/RHSA-2022:1556
https://access.redhat.com/errata/RHSA-2022:1557
https://access.redhat.com/errata/RHSA-2022:1565
https://access.redhat.com/errata/RHSA-2022:1566
https://access.redhat.com/errata/RHSA-2022:1589
https://access.redhat.com/errata/RHSA-2022:1591
https://access.redhat.com/errata/RHSA-2022:1592
https://access.redhat.com/errata/RHSA-2022:1599
https://access.redhat.com/errata/RHSA-2022:1617
https://access.redhat.com/errata/RHSA-2022:1618
https://access.redhat.com/errata/RHSA-2022:1619
https://access.redhat.com/errata/RHSA-2022:1626
https://access.redhat.com/errata/RHSA-2022:1627
https://access.redhat.com/errata/RHSA-2022:1628
https://access.redhat.com/errata/RHSA-2022:1642
https://access.redhat.com/errata/RHSA-2022:1643
https://access.redhat.com/errata/RHSA-2022:1644

10. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.338939
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.488232

11. SonicWall Products

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0036
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0004

12. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20221300-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221303-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221304-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221305-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221306-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221307-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221308-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221312-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221313-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221314-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221315-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221316-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221318-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221320-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221322-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221326-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221329-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221335-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221359-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221369-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221375-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221376-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221396-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221397-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221402-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221407-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221408-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221410-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221411-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221417-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221418-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221427-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221428-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221429-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221430-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221431-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221433-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221434-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221435-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221436-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221437-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221440-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221446-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221447-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221448-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221453-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221454-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221455-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221459-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221461-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221462-1/

https://www.suse.com/support/update/announcement/2022/suse-su-202214943-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214950-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214951-1/

13. Ubuntu

https://ubuntu.com/security/notices/USN-5366-2
https://ubuntu.com/security/notices/USN-5371-2
https://ubuntu.com/security/notices/USN-5376-2
https://ubuntu.com/security/notices/USN-5376-3
https://ubuntu.com/security/notices/USN-5387-1
https://ubuntu.com/security/notices/USN-5388-1
https://ubuntu.com/security/notices/USN-5388-2
https://ubuntu.com/security/notices/USN-5389-1
https://ubuntu.com/security/notices/USN-5390-1
https://ubuntu.com/security/notices/USN-5391-1
https://ubuntu.com/security/notices/USN-5392-1
https://ubuntu.com/security/notices/USN-5394-1
https://ubuntu.com/security/notices/USN-5395-1
https://ubuntu.com/security/notices/USN-5396-1
https://ubuntu.com/security/notices/USN-5397-1
https://ubuntu.com/security/notices/USN-5398-1

Sources of product vulnerability information:

Debian
F5 Products
Huawei
IBM
openSUSE
Oracle Linux
Red Hat
Slackware
SonicWall
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk