GovCERT.HK

Weekly IT Security News Bulletin, 2021-W16

19 April – 25 April 2021

Headlines

Proper identity and access management in cloud environment

- While least privilege principle is widely recognised as a rule of thumb for security, a recent report revealed that many permissions granted and used in cloud infrastructures did not follow this practice and could pose severe security risks such as permission misuse and abuse.

- Permission gaps are common in cloud infrastructures, where some permissions are granted without actually being used. This allows malicious actors (who can be an insider) to exploit the identity with misconfigured permissions and gain access to critical cloud infrastructures or exfiltrate business data. The study found that over 90% of identities were using less than 5% of granted permissions and more than 40% machine identities were inactive.

- It also found that among the more than 40,000 permissions granted to identities across various cloud platforms, about half of them were considered as high risks and could potentially be misused to cause huge damage. Over 85% of enterprises had granted too much permissions to users and allowed them to perform critical functions like destroying and resetting storage and network. Some identities in more than half of the enterprises could even escalate privileges to super admin role.

- Enterprises using cloud infrastructure were remaindered to put in place sufficient control and management of identities and permissions granted in their cloud environment.

Advice

- Always adopt least privilege principle and only grant permissions to users on a need basis.
- Regularly review identities or accounts and remove/suspend those which are inactive or no longer in use.
- Regularly review identity policies and permissions granted to each user.
- Adopt segregation of duties and keep track of permission assignment and usage for better governance.

Sources

- CloudKnox
- Help Net Security

Insufficient patch review in open-source software

- Security researchers conducted an experiment on injecting vulnerable code into an open-source software by submitting patches so as to demonstrate the failure of patch review process of typical open-source projects in identifying the vulnerabilities introduced by malicious developers.

- The study found that due to the openness and complexity of open-source software, malicious developers could circumvent patch review mechanism and introduce stealthy vulnerabilities through a series of minor patches submitted to the code base. Given that a vulnerability requires multiple conditions to be met, an attacker could first identify the immature vulnerabilities and the associated conditions which were not present yet in the software. Malicious patches could then be crafted and used to enable the missing vulnerability conditions. The researchers also suggested some factors that could increase the stealthiness of the vulnerabilities against automatic or manual inspection. In addition to public patch auditing by more developers, the researchers also highlighted that software maintainers should accept preventive patches for high risk immature vulnerabilities in order to mitigate the risks.

- A proof-of-concept of such attack was developed and successfully launched against the Linux kernel project. In response, the project maintainers decided to revert and review all the changes submitted by the affiliated institute of the researchers and ban any future contribution from the institute to the Linux project.

Advice

- Perform testing and verification before accepting the changes in code base.
- Avoid using open-source software which were not properly maintained.
- Apply patches to fix vulnerabilities in a timely manner.

Sources

- Research Paper (Github)
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. CentOS

https://lists.centos.org/pipermail/centos-announce/2021-April/048301.html
https://lists.centos.org/pipermail/centos-announce/2021-April/048302.html

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-auth-bypass-Z3Zze5XC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-cmdinj-nRHKgfHX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-xml-ext-entity-q6Z7uVUg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-cql-inject-c7z9QqyB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-info-disclos-gGvm9Mfu

3. Debian

https://www.debian.org/security/2021/dsa-4892
https://www.debian.org/security/2021/dsa-4893
https://www.debian.org/security/2021/dsa-4894
https://www.debian.org/security/2021/dsa-4895
https://www.debian.org/security/2021/dsa-4898

4. Delta Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-110-03
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-04
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-05

5. Eaton Intelligent Power Manager

https://us-cert.cisa.gov/ics/advisories/icsa-21-110-06

6. F5 Products

https://support.f5.com/csp/article/K01074825
https://support.f5.com/csp/article/K11542555
https://support.f5.com/csp/article/K13290208
https://support.f5.com/csp/article/K61267093

7. Horner Automation Cscape

https://us-cert.cisa.gov/ics/advisories/icsa-21-112-01

8. IBM Products

https://www.ibm.com/support/pages/node/6445481
https://www.ibm.com/support/pages/node/6446219
https://www.ibm.com/support/pages/node/6446277

9. Microsoft Edge (Chromium Based)

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-22-2021

10. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-1206.html
https://linux.oracle.com/errata/ELSA-2021-1297.html
https://linux.oracle.com/errata/ELSA-2021-1298.html
https://linux.oracle.com/errata/ELSA-2021-1301.html
https://linux.oracle.com/errata/ELSA-2021-1307.html

11. Red Hat

https://access.redhat.com/errata/RHSA-2021:1150
https://access.redhat.com/errata/RHSA-2021:1239
https://access.redhat.com/errata/RHSA-2021:1240
https://access.redhat.com/errata/RHSA-2021:1241
https://access.redhat.com/errata/RHSA-2021:1242
https://access.redhat.com/errata/RHSA-2021:1243
https://access.redhat.com/errata/RHSA-2021:1245
https://access.redhat.com/errata/RHSA-2021:1246
https://access.redhat.com/errata/RHSA-2021:1258
https://access.redhat.com/errata/RHSA-2021:1260
https://access.redhat.com/errata/RHSA-2021:1263
https://access.redhat.com/errata/RHSA-2021:1266
https://access.redhat.com/errata/RHSA-2021:1267
https://access.redhat.com/errata/RHSA-2021:1279
https://access.redhat.com/errata/RHSA-2021:1288
https://access.redhat.com/errata/RHSA-2021:1289
https://access.redhat.com/errata/RHSA-2021:1295
https://access.redhat.com/errata/RHSA-2021:1297
https://access.redhat.com/errata/RHSA-2021:1298
https://access.redhat.com/errata/RHSA-2021:1299
https://access.redhat.com/errata/RHSA-2021:1301
https://access.redhat.com/errata/RHSA-2021:1305
https://access.redhat.com/errata/RHSA-2021:1306
https://access.redhat.com/errata/RHSA-2021:1307
https://access.redhat.com/errata/RHSA-2021:1313
https://access.redhat.com/errata/RHSA-2021:1315
https://access.redhat.com/errata/RHSA-2021:1322
https://access.redhat.com/errata/RHSA-2021:1324
https://access.redhat.com/errata/RHSA-2021:1338
https://access.redhat.com/errata/RHSA-2021:1339
https://access.redhat.com/errata/RHSA-2021:1342
https://access.redhat.com/errata/RHSA-2021:1343

12. **Rockwell Automation Stratix Switches**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-110-02

13. **Siemens Mendix**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-110-07

14. **Slackware**

    https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.345522

15. **SUSE**

    https://www.suse.com/support/update/announcement/2021/suse-su-20211238-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211240-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211241-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211242-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211243-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211244-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211245-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211248-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211250-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211251-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211252-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211266-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211267-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211268-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211273-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211274-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211275-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211276-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211277-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211280-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211282-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211292-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211301-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-20211305-1
    https://www.suse.com/support/update/announcement/2021/suse-su-202114700-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-202114702-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-202114704-1/
    https://www.suse.com/support/update/announcement/2021/suse-su-202114705-1/

16. **Symantec Security Analytics**

    https://support.broadcom.com/security-advisory/content/security-advisories/OS-Command-Injection-in-Security-Analytics/SYMSA17969

17. Ubuntu

https://ubuntu.com/security/notices/USN-4563-2
https://ubuntu.com/security/notices/USN-4916-2
https://ubuntu.com/security/notices/USN-4918-1
https://ubuntu.com/security/notices/USN-4918-2
https://ubuntu.com/security/notices/USN-4919-1
https://ubuntu.com/security/notices/USN-4921-1
https://ubuntu.com/security/notices/USN-4922-1
https://ubuntu.com/security/notices/USN-4923-1
https://ubuntu.com/security/notices/USN-4924-1
https://ubuntu.com/security/notices/USN-4925-1

18. VMware

https://www.vmware.com/security/advisories/VMSA-2021-0006.html

19. Wireshark

https://www.wireshark.org/security/wnpa-sec-2021-03.html

Sources of product vulnerability information:

Broadcom
CentOS
Cisco
Debian
F5
IBM
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
VMware
Wireshark

Contact:

cert@govcert.gov.hk