GovCERT.HK

Weekly IT Security News Bulletin, 2021-W40

4 October – 10 October 2021

Headlines

Python ransomware targeting virtual machines hypervisors

- A recent investigation into a ransomware attack revealed that attackers were using a custom Python script to encrypt virtual machines and disks hosted on VMware ESXi servers to disrupt the organisation's infrastructure.

- According to the investigation result, the attacker remotely accessed and controlled a computer assigned to a user with Active Directory administrator privileges. To gain the initial foothold of the target network, the attacker was likely to use a brute-force attack to take control the account of a remote access service. Subsequently, the attacker identified virtual machines hypervisors in the network and uploaded the Python ransomware. The attacker only spent around three hours to deploy the ransomware scripts from the time of the initial compromise.

- VMware ESXi servers represent an attractive target for ransomware threat actors as compromising a single ESXi server can beat multiple virtual machines at once and eventually produce rapid and disruptive impact.

Advice

- Stay aware of the latest trends and imminent threats of ransomware and adopt security measures to mitigate the risks.
- Adopt two-factor authentication for remote access and privileged accounts.
- Deploy virtual private networks with strong authentication for remote access from the Internet.

Sources

- Sophos
- ZDNet

Popular streaming platform suffered massive data breach

- A popular streaming platform suffered a massive data breach where sensitive data of the platform was allegedly leaked online. According to the announcement made, the breach was caused by a server misconfiguration that leads to unauthorised data access.

- A post on an online forum indicates that over 125 GB of data was leaked. The leaked data includes user payment reports, as well as the platform's program source code, software development kits (SDKs) and internal security tools. Although no user credential was found in the leak, the platform has reset the stream keys of all users in response to the data leakage incident.

- While the full extent of the breach is still under investigation, the source of the leak was believed to be an internal Git server. Git servers was a distributed version control system for program development and were commonly deployed for programmers to make controlled and reversible changes on source code repositories.

Advice

- Conduct periodic vulnerability scanning and configuration review to mitigate the security risks due to misconfigured infrastructure and system components.
- Monitor network for suspicious network activities, especially abnormal outbound data transfer.
- Implement both storage encryption and data tokenisation for multiple layers of protection against various attack vectors.
- Consumers should be aware of the risks involved when providing their personal information to service providers and should adopt multi-factor authentication whenever available to access online services.

Sources

- Twitch
- Bleeping Computer
- The Record
- ZDNet

Product Vulnerability Notes & Security Updates

1. **Android**

   https://source.android.com/security/bulletin/2021-10-01

2. **Apache OpenOffice**

   https://www.openoffice.org/security/cves/CVE-2021-28129.html
   https://www.openoffice.org/security/cves/CVE-2021-33035.html
   https://www.openoffice.org/security/cves/CVE-2021-40439.html

3. **Boston Scientific Zoom Latitude**

   https://us-cert.cisa.gov/ics/advisories/icsma-21-273-01

4. **Debian**

   https://www.debian.org/security/2021/dsa-4979
   https://www.debian.org/security/2021/dsa-4980
   https://www.debian.org/security/2021/dsa-4981

5. **Emerson WirelessHART Gateway**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02

6. **F5 Products**

   https://support.f5.com/csp/article/K19559038
   https://support.f5.com/csp/article/K55834441

7. **FATEK Automation Products**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-280-06
   https://us-cert.cisa.gov/ics/advisories/icsa-21-280-07

8. **Fortinet**

   https://www.fortiguard.com/psirt/FG-IR-20-027
   https://www.fortiguard.com/psirt/FG-IR-20-072
   https://www.fortiguard.com/psirt/FG-IR-20-074
   https://www.fortiguard.com/psirt/FG-IR-20-098
   https://www.fortiguard.com/psirt/FG-IR-20-183
   https://www.fortiguard.com/psirt/FG-IR-20-234
   https://www.fortiguard.com/psirt/FG-IR-21-112

9. **Honeywell Experion PKS and ACE Controllers**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-278-04

10. **Huawei Products**

    https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210929-01-auth-en

11. **InHand Networks IR615 Router**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-280-05

12. **Johnson Controls exacqVision Products**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-280-01
    https://us-cert.cisa.gov/ics/advisories/icsa-21-280-03

13. **McAfee**

    https://kc.mcafee.com/corporate/index?page=content&id=SB10361

14. **Mitsubishi Electric Products**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-278-01
    https://us-cert.cisa.gov/ics/advisories/icsa-21-280-04

15. **Mobile Industrial Robots Vehicles and MiR Fleet Software**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-280-02

16. **Moxa MXview Network Management Software**

    https://us-cert.cisa.gov/ics/advisories/icsa-21-278-03

17. **openSUSE**

    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/2AYA6VEHMLTAF6FDL4C6CPC73YV5SVJY/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4WV4L3BNHGJFK3NT7YVDUR6UNHPAFSZC/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5EY52N4KALEDKULS6YHUPW2C7OJTGHTS/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/32OSJUOT5EKYB352W3UZ3NLUB6N4FXCT/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FWIIK75CV5Y6TWUXN67IYXFNHIHRZSXN/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/OT7AMKZYZG3NMSSJK4GVQCGFPLIGSKD5/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ROJISG4GC22MLBYTQB5THWN4V2IFZC7P/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/TYMYANBGPUFKQ7SIIB3PZLAAR35QYXOR/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/VUBHGD7IXTYDS4PM3AVFQLIU2HR2Y24Y/
    https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/VXUBRXLMWBRLT5YI5UGAWTWUKG3VAM46/

18. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-9470.html
https://linux.oracle.com/errata/ELSA-2021-9471.html

19. Red Hat

https://access.redhat.com/errata/RHSA-2021:3646
https://access.redhat.com/errata/RHSA-2021:3676
https://access.redhat.com/errata/RHSA-2021:3700
https://access.redhat.com/errata/RHSA-2021:3703
https://access.redhat.com/errata/RHSA-2021:3704
https://access.redhat.com/errata/RHSA-2021:3723
https://access.redhat.com/errata/RHSA-2021:3724
https://access.redhat.com/errata/RHSA-2021:3725
https://access.redhat.com/errata/RHSA-2021:3733
https://access.redhat.com/errata/RHSA-2021:3741
https://access.redhat.com/errata/RHSA-2021:3743
https://access.redhat.com/errata/RHSA-2021:3745
https://access.redhat.com/errata/RHSA-2021:3746
https://access.redhat.com/errata/RHSA-2021:3748

20. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.434604

21. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20213201-2/
https://www.suse.com/support/update/announcement/2021/suse-su-20213267-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213268-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213269-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213277-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213282-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213289-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213290-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213291-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213292-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213293-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213294-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213295-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213296-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213297-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213298-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213299-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213300-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213301-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213322-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114821-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114822-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114823-1/

22. Trend Micro

https://success.trendmicro.com/solution/000289183

23. Ubuntu

https://ubuntu.com/security/notices/USN-4973-2
https://ubuntu.com/security/notices/USN-5022-3
https://ubuntu.com/security/notices/USN-5091-2
https://ubuntu.com/security/notices/USN-5094-2
https://ubuntu.com/security/notices/USN-5097-1
https://ubuntu.com/security/notices/USN-5098-1
https://ubuntu.com/security/notices/USN-5099-1
https://ubuntu.com/security/notices/USN-5100-1
https://ubuntu.com/security/notices/USN-5101-1
https://ubuntu.com/security/notices/USN-5102-1
https://ubuntu.com/security/notices/USN-5103-1
https://ubuntu.com/security/notices/USN-5104-1
https://ubuntu.com/security/notices/USN-5105-1
https://ubuntu.com/security/notices/USN-5106-1
https://ubuntu.com/security/notices/USN-5107-1

24. Xen

https://xenbits.xen.org/xsa/advisory-386.html

Sources of product vulnerability information:

Android
Debian
F5 Products
Fortinet
Huawei
McAfee
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk