GovCERT.HK

Weekly IT Security News Bulletin, 2020-W36

31 August –6 September 2020

Headlines

Ransomware attacks with penetration testing tools

- Researchers observed that ransomware kept being the major cyber threat over the last five quarters. There is also a growing trend that attackers abuse common penetration testing tools to conduct ransomware attacks. This is in contrast with traditional ransomware attacks in which trojans like Emotet and Trickbot are deployed to steal data and hold hostage of it.

- Cobalt Strike is a popular penetration testing tool that is packed into attackers' toolbox. In the last quarter, almost two-thirds of ransomware attacks involved Cobalt Strike as an intrusion tool for gaining access into remote hosts and moving across the local area network to infect other computers.

- In a case of ransomware infection, a Cobalt Strike server was adopted for command and control of the attack. The attacker executed another hacking tool called "CrackMapExecWin" to trigger a Windows Group Policy update on different networks of the victim. The Group Policy would create a Windows service to run ransomware on the infected hosts. User accounts would also be created by the attacker to establish remote desktop connections to other targeted servers on the network.

Advice

- Patch your systems timely to avoid being exploited by the penetration testing tools.

- Conduct regular penetration tests on your networks and systems to look for any loopholes to be fixed.

- Monitor your network and server logs for suspicious activities such as unexpected remote accesses, group policy settings, or user account creations.

Sources

- Talos
- TechRepublic

Blocking Internet access to unsafe network services

- After assessing millions of Internet-facing systems of about 40,000 commercial and public sector organisations, a research team of a US security company revealed that 33% of the organisations and 0.4% of their systems exposed at least one unsafe network services to the Internet.

- The exposed services included data storage, remote access, and network access among others. The research highlighted the correlation between service exposure and broader security issues such as unpatched software and lack of web encryption. The impact got even worse if vendors and business partners in the digital supply chain had unsafe network services, which would further put their customers at risk.

- Blocking Internet access to unsafe network services is regarded as a fundamental security hygiene practice. The finding of a high percentage of suppliers that failed to follow the best practice serves a warning shot for management teams. They should act promptly for mitigating security risks brought from third parties in the supply chain.

Advice

- Close all unnecessary network ports on your systems and protect those ports in use with additional security controls such as virtual private networks, multi-factor authentication or IP address whitelisting whenever applicable.

- Scan your networks periodically for open ports to detect potential misconfigurations.

- Assess the risks brought from third parties in the digital supply chain before adopting the relevant digital services.

Sources

- RiskRecon
- Help Net Security
- Infosecurity

Product Vulnerability Notes & Security Updates

1. CentOS

https://lists.centos.org/pipermail/centos-announce/2020-September/035805.html
https://lists.centos.org/pipermail/centos-announce/2020-September/035806.html

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-info-disclosure-vMJMMgJ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-tls-dos-xW53TBhb
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-buffer-cSdmfWUt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-cli-privescl-sDVEmhqv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-LJtNFjeN
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-G3NSjPn7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ttcgB9R3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-UyTKCPGg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-vY8M4KGB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-file-overwrite-UONzPMkr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-path-emy79OC2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-osinj-rce-pwTkPCJv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-wsa-esa-info-dis-vsvPzOHP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-media-znjfwHD6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-meetings-UtbwOR4Q

3. Debian

https://www.debian.org/security/2020/dsa-4753
https://www.debian.org/security/2020/dsa-4755
https://www.debian.org/security/2020/dsa-4756
https://www.debian.org/security/2020/dsa-4757

4. F5 Products

https://support.f5.com/csp/article/K38481791

5. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-20:24.ipv6.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-20:25.sctp.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-20:26.dhclient.asc

6. Gentoo Linux

https://security.gentoo.org/glsa/202008-19
https://security.gentoo.org/glsa/202008-20
https://security.gentoo.org/glsa/202008-21
https://security.gentoo.org/glsa/202008-22
https://security.gentoo.org/glsa/202008-23
https://security.gentoo.org/glsa/202008-24

7. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200902-01-command-en

8. Mitsubishi Electric Products

https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01

9. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00065.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00066.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00067.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00068.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00069.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00070.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00071.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00072.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00073.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00074.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00075.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00076.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00000.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00001.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00002.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00003.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00004.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00005.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00006.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00007.html
https://lists.opensuse.org/opensuse-security-announce/2020-09/msg00008.html

10. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-3557.html
https://linux.oracle.com/errata/ELSA-2020-5827.html
https://linux.oracle.com/errata/ELSA-2020-5828.html

11. Red Hat

https://access.redhat.com/errata/RHSA-2020:3539
https://access.redhat.com/errata/RHSA-2020:3579
https://access.redhat.com/errata/RHSA-2020:3580
https://access.redhat.com/errata/RHSA-2020:3581
https://access.redhat.com/errata/RHSA-2020:3585
https://access.redhat.com/errata/RHSA-2020:3586
https://access.redhat.com/errata/RHSA-2020:3587
https://access.redhat.com/errata/RHSA-2020:3588
https://access.redhat.com/errata/RHSA-2020:3598
https://access.redhat.com/errata/RHSA-2020:3600
https://access.redhat.com/errata/RHSA-2020:3601
https://access.redhat.com/errata/RHSA-2020:3602

12. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20202360-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202373-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202391-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202398-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202399-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202401-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202403-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202404-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202405-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202407-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202408-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202409-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202442-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202443-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202444-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202445-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202446-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202450-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202452-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202453-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202455-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202456-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202461-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014475-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014481-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014482-1/

13. Ubuntu

https://ubuntu.com/security/notices/USN-4449-2
https://ubuntu.com/security/notices/USN-4471-2
https://ubuntu.com/security/notices/USN-4478-1
https://ubuntu.com/security/notices/USN-4479-1
https://ubuntu.com/security/notices/USN-4480-1
https://ubuntu.com/security/notices/USN-4481-1
https://ubuntu.com/security/notices/USN-4482-1
https://ubuntu.com/security/notices/USN-4483-1
https://ubuntu.com/security/notices/USN-4484-1
https://ubuntu.com/security/notices/USN-4485-1
https://ubuntu.com/security/notices/USN-4486-1
https://ubuntu.com/security/notices/USN-4487-1
https://ubuntu.com/security/notices/USN-4488-1

Sources of product vulnerability information:

CentOS
Cisco
Debian
F5
FreeBSD
Gentoo Linux
Huawei
openSUSE
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk