GovCERT.HK

Weekly IT Security News Bulletin, 2020-W46

9 November – 15 November 2020

Headlines

Do not reuse your passwords

- A recent survey reveals that employee negligence is the major cause of data breaches where 63% employees reuse the same passwords for different accounts on work devices. While employees are provided with work devices for remote work during epidemic, they usually put their personal data on the device and 63% of them have no concern about that.

- While it is a tendency for users to use one single password rather than multiple passwords for different accounts, password reuse poses a serious security risk and lead to compromise of account and data breach. By taking over one account of the user, the hacker can use the credential obtained to compromise other accounts (i.e., credential stuffing). Although users may find it difficult to remember a complex password for each of their many accounts, they can always get help from password management tools.

- The use of work devices for personal activities can increase the chance of cyber attack. The situation can be even worse when users apply the same password for their personal and work accounts. Corporate data and systems can be at stake as a result.

Advice

- Enforce password policy to ensure strong and unique password for every account.
- Apply two-factor authentication to reduce the chance of account being compromised.
- Educate users on good cyber hygiene, especially on password management best practices.

Sources

- InfoSecurity
- Visual Objects

DNS cache poisoning

- A group of researchers demonstrated a technique called "Side-channel Attacked DNS" to redirect traffic from the destinated domain to another one in order to perform eavesdropping or tempering. This can be done by injecting malicious DNS records into the cache of DNS resolvers.

- The DNS cache is commonly used to allow DNS resolvers to quickly response to a domain name resolution request by returning the cached result from previous requests on the same domain name. Without proper authentication, a hacker can impersonate the authoritative server and return malicious results to resolvers and redirect users to malicious sites.

- DNS cache poisoning was once fixed by increasing the difficulty in guessing the correct transaction ID which is required for verification of the DNS response. The researchers exploit a side channel by flooding a DNS resolver with many responses that are spoofed to be from the name server of a target domain. In the process, they managed to identify the right source port used to initiate a DNS query based on the ICMP responses received from the DNS resolver and significantly reduce the search space for the transaction ID.

- More than 34% open resolvers on the Internet are found to be vulnerable and operating systems like Linux, Windows, MacOS and FreeBSD are also affected.

Advice

- Adopt Domain Name System Security Extensions (DNSSEC) to provide authentication on DNS data exchange.
- Disable outgoing ICMP replies to avoid inferring of the source port of DNS queries.
- Set a short period for timeout for DNS queries to avoid brute-force of source port and injection of malicious responses.

Sources

- The Hacker News
- Ars Technica

Product Vulnerability Notes & Security Updates

1. Apache OpenOffice

https://www.openoffice.org/security/cves/CVE-2020-13958.html

2. Apple Products

https://support.apple.com/zh-tw/HT211931
https://support.apple.com/zh-tw/HT211934
https://support.apple.com/zh-tw/HT211946

3. CentOS

https://lists.centos.org/pipermail/centos-announce/2020-November/035810.html
https://lists.centos.org/pipermail/centos-announce/2020-November/035811.html
https://lists.centos.org/pipermail/centos-announce/2020-November/035812.html
https://lists.centos.org/pipermail/centos-announce/2020-November/035813.html
https://lists.centos.org/pipermail/centos-announce/2020-November/035814.html
https://lists.centos.org/pipermail/centos-announce/2020-November/035816.html
https://lists.centos.org/pipermail/centos-announce/2020-November/035817.html

4. Cisco IOS XR Software

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cp-dos-ej8VB9QY

5. Citrix Products

https://support.citrix.com/article/CTX285059
https://support.citrix.com/article/CTX285061

6. Debian

https://www.debian.org/security/2020/dsa-4784
https://www.debian.org/security/2020/dsa-4785
https://www.debian.org/security/2020/dsa-4786
https://www.debian.org/security/2020/dsa-4787
https://www.debian.org/security/2020/dsa-4788
https://www.debian.org/security/2020/dsa-4789

7. Gentoo Linux

https://security.gentoo.org/glsa/202011-06
https://security.gentoo.org/glsa/202011-07
https://security.gentoo.org/glsa/202011-08
https://security.gentoo.org/glsa/202011-09
https://security.gentoo.org/glsa/202011-10
https://security.gentoo.org/glsa/202011-11
https://security.gentoo.org/glsa/202011-12
https://security.gentoo.org/glsa/202011-13
https://security.gentoo.org/glsa/202011-14

8. Google Chrome

https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_9.html
https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_11.html

9. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201111-02-dos-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201111-02-injection-en

10. IBM InfoSphere Information Server

https://www.ibm.com/support/pages/node/6351229
https://www.ibm.com/support/pages/node/6366715

11. Intel Products

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00262.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00350.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00358.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00360.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00362.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00368.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00380.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00381.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00388.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00389.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00390.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00391.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00398.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00400.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00402.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00403.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00408.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00409.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00410.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00412.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00413.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00414.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00415.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00416.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00417.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00418.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00419.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00420.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00421.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00422.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00423.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00424.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00427.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00429.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00430.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00431.html

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00439.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00446.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00447.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00449.html

12. McAfee Products

https://kc.mcafee.com/corporate/index?page=content&id=SB10334
https://kc.mcafee.com/corporate/index?page=content&id=SB10335

13. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00026.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00027.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00028.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00029.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00030.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00031.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00032.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00033.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00034.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00035.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00036.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00037.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00038.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00041.html
https://www.suse.com/support/update/announcement/2020/suse-su-20203261-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203262-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203263-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203264-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203268-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203269-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203271-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203272-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203273-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203274-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203275-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203276-1/

14. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-4432.html
https://linux.oracle.com/errata/ELSA-2020-4433.html
https://linux.oracle.com/errata/ELSA-2020-4436.html
https://linux.oracle.com/errata/ELSA-2020-4442.html
https://linux.oracle.com/errata/ELSA-2020-4443.html
https://linux.oracle.com/errata/ELSA-2020-4444.html
https://linux.oracle.com/errata/ELSA-2020-4445.html
https://linux.oracle.com/errata/ELSA-2020-4451.html
https://linux.oracle.com/errata/ELSA-2020-4453.html
https://linux.oracle.com/errata/ELSA-2020-4464.html
https://linux.oracle.com/errata/ELSA-2020-4465.html

https://linux.oracle.com/errata/ELSA-2020-4469.html
https://linux.oracle.com/errata/ELSA-2020-4479.html
https://linux.oracle.com/errata/ELSA-2020-4482.html
https://linux.oracle.com/errata/ELSA-2020-4483.html
https://linux.oracle.com/errata/ELSA-2020-4484.html
https://linux.oracle.com/errata/ELSA-2020-4490.html
https://linux.oracle.com/errata/ELSA-2020-4497.html
https://linux.oracle.com/errata/ELSA-2020-4500.html
https://linux.oracle.com/errata/ELSA-2020-4508.html
https://linux.oracle.com/errata/ELSA-2020-4514.html
https://linux.oracle.com/errata/ELSA-2020-4539.html
https://linux.oracle.com/errata/ELSA-2020-4542.html
https://linux.oracle.com/errata/ELSA-2020-4545.html
https://linux.oracle.com/errata/ELSA-2020-4547.html
https://linux.oracle.com/errata/ELSA-2020-4553.html
https://linux.oracle.com/errata/ELSA-2020-4568.html
https://linux.oracle.com/errata/ELSA-2020-4599.html
https://linux.oracle.com/errata/ELSA-2020-4619.html
https://linux.oracle.com/errata/ELSA-2020-4625.html
https://linux.oracle.com/errata/ELSA-2020-4627.html
https://linux.oracle.com/errata/ELSA-2020-4628.html
https://linux.oracle.com/errata/ELSA-2020-4629.html
https://linux.oracle.com/errata/ELSA-2020-4634.html
https://linux.oracle.com/errata/ELSA-2020-4638.html
https://linux.oracle.com/errata/ELSA-2020-4643.html
https://linux.oracle.com/errata/ELSA-2020-4647.html
https://linux.oracle.com/errata/ELSA-2020-4649.html
https://linux.oracle.com/errata/ELSA-2020-4650.html
https://linux.oracle.com/errata/ELSA-2020-4655.html
https://linux.oracle.com/errata/ELSA-2020-4659.html
https://linux.oracle.com/errata/ELSA-2020-4667.html
https://linux.oracle.com/errata/ELSA-2020-4682.html
https://linux.oracle.com/errata/ELSA-2020-4687.html
https://linux.oracle.com/errata/ELSA-2020-4689.html
https://linux.oracle.com/errata/ELSA-2020-4690.html
https://linux.oracle.com/errata/ELSA-2020-4697.html
https://linux.oracle.com/errata/ELSA-2020-4709.html
https://linux.oracle.com/errata/ELSA-2020-4751.html
https://linux.oracle.com/errata/ELSA-2020-4756.html
https://linux.oracle.com/errata/ELSA-2020-4760.html
https://linux.oracle.com/errata/ELSA-2020-4763.html
https://linux.oracle.com/errata/ELSA-2020-4766.html
https://linux.oracle.com/errata/ELSA-2020-4799.html
https://linux.oracle.com/errata/ELSA-2020-4805.html
https://linux.oracle.com/errata/ELSA-2020-4806.html
https://linux.oracle.com/errata/ELSA-2020-4807.html
https://linux.oracle.com/errata/ELSA-2020-4820.html
https://linux.oracle.com/errata/ELSA-2020-4827.html
https://linux.oracle.com/errata/ELSA-2020-4946.html
https://linux.oracle.com/errata/ELSA-2020-4953.html
https://linux.oracle.com/errata/ELSA-2020-5002.html
https://linux.oracle.com/errata/ELSA-2020-5003.html
https://linux.oracle.com/errata/ELSA-2020-5010.html

https://linux.oracle.com/errata/ELSA-2020-5011.html
https://linux.oracle.com/errata/ELSA-2020-5012.html
https://linux.oracle.com/errata/ELSA-2020-5020.html
https://linux.oracle.com/errata/ELSA-2020-5021.html
https://linux.oracle.com/errata/ELSA-2020-5023.html
https://linux.oracle.com/errata/ELSA-2020-5040.html
https://linux.oracle.com/errata/ELSA-2020-5913.html
https://linux.oracle.com/errata/ELSA-2020-5914.html
https://linux.oracle.com/errata/ELSA-2020-5917.html
https://linux.oracle.com/errata/ELSA-2020-5923.html
https://linux.oracle.com/errata/ELSA-2020-5924.html
https://linux.oracle.com/errata/ELSA-2020-5926.html

15. Red Hat

https://access.redhat.com/errata/RHSA-2020:4379
https://access.redhat.com/errata/RHSA-2020:4974
https://access.redhat.com/errata/RHSA-2020:4978
https://access.redhat.com/errata/RHSA-2020:4990
https://access.redhat.com/errata/RHSA-2020:4991
https://access.redhat.com/errata/RHSA-2020:4992
https://access.redhat.com/errata/RHSA-2020:4999
https://access.redhat.com/errata/RHSA-2020:5002
https://access.redhat.com/errata/RHSA-2020:5003
https://access.redhat.com/errata/RHSA-2020:5004
https://access.redhat.com/errata/RHSA-2020:5009
https://access.redhat.com/errata/RHSA-2020:5010
https://access.redhat.com/errata/RHSA-2020:5011
https://access.redhat.com/errata/RHSA-2020:5012
https://access.redhat.com/errata/RHSA-2020:5020
https://access.redhat.com/errata/RHSA-2020:5021
https://access.redhat.com/errata/RHSA-2020:5023
https://access.redhat.com/errata/RHSA-2020:5026
https://access.redhat.com/errata/RHSA-2020:5040
https://access.redhat.com/errata/RHSA-2020:5050
https://access.redhat.com/errata/RHSA-2020:5054
https://access.redhat.com/errata/RHSA-2020:5055
https://access.redhat.com/errata/RHSA-2020:5056
https://access.redhat.com/errata/RHSA-2020:5079
https://access.redhat.com/errata/RHSA-2020:5083
https://access.redhat.com/errata/RHSA-2020:5084
https://access.redhat.com/errata/RHSA-2020:5085
https://access.redhat.com/errata/RHSA-2020:5086
https://access.redhat.com/errata/RHSA-2020:5099
https://access.redhat.com/errata/RHSA-2020:5100
https://access.redhat.com/errata/RHSA-2020:5104

16. Siemens SCALANCE W 1750D

https://us-cert.cisa.gov/ics/advisories/icsa-20-315-05

17. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20203204-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203210-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203219-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203222-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203225-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203230-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203231-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203235-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203243-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203244-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203245-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203250-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203251-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203255-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203256-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203257-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203279-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203281-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203282-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203283-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203292-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203310-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203311-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203312-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203313-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203314-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203315-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014535-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014537-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014538-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014540-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014541-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014542-1/

18. Ubuntu

https://ubuntu.com/security/notices/USN-4171-6
https://ubuntu.com/security/notices/USN-4607-2
https://ubuntu.com/security/notices/USN-4621-1
https://ubuntu.com/security/notices/USN-4622-1
https://ubuntu.com/security/notices/USN-4622-2
https://ubuntu.com/security/notices/USN-4623-1
https://ubuntu.com/security/notices/USN-4624-1
https://ubuntu.com/security/notices/USN-4625-1
https://ubuntu.com/security/notices/USN-4626-1
https://ubuntu.com/security/notices/USN-4627-1
https://ubuntu.com/security/notices/USN-4628-1
https://ubuntu.com/security/notices/USN-4628-2
https://ubuntu.com/security/notices/USN-4629-1
https://ubuntu.com/security/notices/USN-4630-1
https://ubuntu.com/security/notices/USN-4631-1

https://ubuntu.com/security/notices/USN-4632-1

Sources of product vulnerability information:

Apple
CentOS
Cisco
Citrix
Debian
Gentoo Linux
Google Chrome
Huawei
IBM
Intel
McAfee
OpenOffice
openSUSE
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk