GovCERT.HK

Weekly IT Security News Bulletin, 2020-W45

2 November – 8 November 2020

Headlines

Patch your chrome browser now

- Google has released updates to fix several vulnerabilities in the Chrome browser, including two which are being actively exploited in attacks.
- The first vulnerability (CVE-2020-16009) is related to inappropriate implementation of the V8 JavaScript engine, which can be exploited through specially crafted HTML page to corrupt memory. It allows attacker to remotely execute arbitrary code by enticing victims to open the webpage.
- The second vulnerability (CVE-2020-16010) is related to heap-based buffer flow in the UI on Android, which allows attackers to escalate privileges in Chrome's sandbox through specially crafted HTML pages.
- Google also disclosed that attackers are actively exploiting a vulnerability in the Windows kernel (CVE-2020-17087) through a vulnerability in Chrome (CVE-2020-15999), where the latter has already been patched in late October. Similar to the second vulnerability mentioned above, it allows execution of code outside Chrome's sandbox through the flaw of heap buffer overflow in the implementation of FreeType. The patch for CVE-2020-17087 is not yet available but expected to be released in upcoming Microsoft's monthly patch.

Advice

- Apply patches on browsers and operating systems in a timely manner.
- Do not visit suspicious webpages or open links from untrusted sources.

Sources

- Threatpost
- SecurityWeek
- DarkReading

Remote attack on internal networks

- Network address translation (NAT) is a process to map a single public IP address to multiple devices within an internal network. Some may think that NAT helps improve security as the internal devices cannot be reached directly from the Internet (and malicious actors) and only connections initiated from the internal network are allowed.

- However, a security researcher demonstrated a technique to launch a browser-based attack to obtain remote access to services on a victim's device within an internal network. As a prerequisite of the attack, the victim's device has to support application-layer gateway which is used to manage connections between the public and internal network services to enable NAT traversal for different protocols.

- By exploiting vulnerable web browsers on the victim's machine in the internal network, attackers can load malicious code for identifying internal IP addresses through the web real time communications protocol. After that, attackers can generate a session initiation protocol registration packet for VoIP call set up and establish two-way communications with specific ports (or services) on devices within the internal network. Such direct connection from the external network can expose the internal devices and services to cyber attacks.

Advice

- Never assume that devices within an internal network are immune from cyber attacks.
- Segment the network to reduce impact and surface for attacks through any compromised device within a network.
- Disable ports and services that are not in use.
- Always patch your browsers in a timely manner

Sources

- iTnews
- SecurityWeek
- NAT Slipstreaming

Product Vulnerability Notes & Security Updates

1. Android

https://source.android.com/security/bulletin/2020-11-01

2. Apple macOS Catalina

https://support.apple.com/zh-tw/HT211947

3. ARC Informatique PcVue

https://us-cert.cisa.gov/ics/advisories/icsa-20-308-03

4. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-file-read-LsvDD6Uh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cedge-filt-bypass-Y6wZMqm4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-zWkppJxL
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CIMC-CIV-pKDBe9x5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-enum-CyheP3B7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-eff-incperm-9E6h4yBz
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-zip-bypass-gbU4gtTg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-dos-uTx2dqu2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pxe-unsign-code-exec-qAa78fD2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-fNZX8hHj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-euRCwX9
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxs-pkjCmq9d
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tele-info-DrEGLpDQ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepegr-4xynYLUj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepescm-BjgQm4vJ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepeshlg-tJghOQcA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepestd-8C3J9Vc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-traversal-hQh24tmk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-escalation-Jhqs5Skf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-file-Y2JSRNRb
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-privilege-zPmMf73k
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanpt2-FqLuefsS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanuafw-ZHkdGGEy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanx2-KpFVSUc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanx3-vrZbOqqD
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanxss1-XhJCymBt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanxss2-ugJyqxWF

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanxsshi-9KHEqRpM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmxss2-NL4KSSVR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-flood-dos-YnU9EXOv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vsoln-arbfile-gtsEYxns
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-nbr-NOS6FQ24
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-teams-xss-zLW9tD3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-vdi-qQrpBwuJ

5. Debian

https://www.debian.org/security/2020/dsa-4782
https://www.debian.org/security/2020/dsa-4783

6. F5 Products

https://support.f5.com/csp/article/K03125360
https://support.f5.com/csp/article/K20059815
https://support.f5.com/csp/article/K21540525
https://support.f5.com/csp/article/K32055534
https://support.f5.com/csp/article/K43310520
https://support.f5.com/csp/article/K53821711
https://support.f5.com/csp/article/K57274211
https://support.f5.com/csp/article/K75111593
https://support.f5.com/csp/article/K82530456

7. Fortinet Products

https://www.fortiguard.com/psirt/FG-IR-20-044
https://www.fortiguard.com/psirt/FG-IR-20-105

8. Gentoo Linux

https://security.gentoo.org/glsa/202011-01
https://security.gentoo.org/glsa/202011-02
https://security.gentoo.org/glsa/202011-03
https://security.gentoo.org/glsa/202011-04
https://security.gentoo.org/glsa/202011-05

9. Google Chrome

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

10. Huawei FusionCompute

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201104-01-encryption-en

11. Mitsubishi Products

https://us-cert.cisa.gov/ics/advisories/icsa-20-161-02
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04
https://us-cert.cisa.gov/ics/advisories/icsa-20-310-02

12. Mozilla VPN

https://www.mozilla.org/en-US/security/advisories/mfsa2020-48/

13. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00072.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00073.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00074.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00075.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00076.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00077.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00078.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00079.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00080.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00081.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00000.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00001.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00002.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00003.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00004.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00005.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00006.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00007.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00008.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00009.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00010.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00011.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00012.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00013.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00014.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00015.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00016.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00017.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00018.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00019.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00020.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00021.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00022.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00023.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00024.html
https://lists.opensuse.org/opensuse-security-announce/2020-11/msg00025.html

14. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-4907.html
https://linux.oracle.com/errata/ELSA-2020-4908.html
https://linux.oracle.com/errata/ELSA-2020-4910.html
https://linux.oracle.com/errata/ELSA-2020-5906.html
https://linux.oracle.com/errata/ELSA-2020-5912.html

15. QNAP Products

https://www.qnap.com/en/security-advisory/qsa-20-10
https://www.qnap.com/en/security-advisory/qsa-20-11

16. Red Hat

https://access.redhat.com/errata/RHSA-2020:4431
https://access.redhat.com/errata/RHSA-2020:4432
https://access.redhat.com/errata/RHSA-2020:4433
https://access.redhat.com/errata/RHSA-2020:4436
https://access.redhat.com/errata/RHSA-2020:4442
https://access.redhat.com/errata/RHSA-2020:4443
https://access.redhat.com/errata/RHSA-2020:4444
https://access.redhat.com/errata/RHSA-2020:4445
https://access.redhat.com/errata/RHSA-2020:4451
https://access.redhat.com/errata/RHSA-2020:4453
https://access.redhat.com/errata/RHSA-2020:4464
https://access.redhat.com/errata/RHSA-2020:4465
https://access.redhat.com/errata/RHSA-2020:4469
https://access.redhat.com/errata/RHSA-2020:4479
https://access.redhat.com/errata/RHSA-2020:4481
https://access.redhat.com/errata/RHSA-2020:4482
https://access.redhat.com/errata/RHSA-2020:4483
https://access.redhat.com/errata/RHSA-2020:4484
https://access.redhat.com/errata/RHSA-2020:4490
https://access.redhat.com/errata/RHSA-2020:4497
https://access.redhat.com/errata/RHSA-2020:4508
https://access.redhat.com/errata/RHSA-2020:4514
https://access.redhat.com/errata/RHSA-2020:4539
https://access.redhat.com/errata/RHSA-2020:4542
https://access.redhat.com/errata/RHSA-2020:4545
https://access.redhat.com/errata/RHSA-2020:4547
https://access.redhat.com/errata/RHSA-2020:4553
https://access.redhat.com/errata/RHSA-2020:4568
https://access.redhat.com/errata/RHSA-2020:4599
https://access.redhat.com/errata/RHSA-2020:4605
https://access.redhat.com/errata/RHSA-2020:4609
https://access.redhat.com/errata/RHSA-2020:4619
https://access.redhat.com/errata/RHSA-2020:4625
https://access.redhat.com/errata/RHSA-2020:4627
https://access.redhat.com/errata/RHSA-2020:4628
https://access.redhat.com/errata/RHSA-2020:4629
https://access.redhat.com/errata/RHSA-2020:4634
https://access.redhat.com/errata/RHSA-2020:4638
https://access.redhat.com/errata/RHSA-2020:4641
https://access.redhat.com/errata/RHSA-2020:4643
https://access.redhat.com/errata/RHSA-2020:4647
https://access.redhat.com/errata/RHSA-2020:4649
https://access.redhat.com/errata/RHSA-2020:4650
https://access.redhat.com/errata/RHSA-2020:4654
https://access.redhat.com/errata/RHSA-2020:4655
https://access.redhat.com/errata/RHSA-2020:4659

https://access.redhat.com/errata/RHSA-2020:4667
https://access.redhat.com/errata/RHSA-2020:4670
https://access.redhat.com/errata/RHSA-2020:4676
https://access.redhat.com/errata/RHSA-2020:4682
https://access.redhat.com/errata/RHSA-2020:4685
https://access.redhat.com/errata/RHSA-2020:4686
https://access.redhat.com/errata/RHSA-2020:4687
https://access.redhat.com/errata/RHSA-2020:4689
https://access.redhat.com/errata/RHSA-2020:4690
https://access.redhat.com/errata/RHSA-2020:4694
https://access.redhat.com/errata/RHSA-2020:4697
https://access.redhat.com/errata/RHSA-2020:4709
https://access.redhat.com/errata/RHSA-2020:4712
https://access.redhat.com/errata/RHSA-2020:4743
https://access.redhat.com/errata/RHSA-2020:4751
https://access.redhat.com/errata/RHSA-2020:4756
https://access.redhat.com/errata/RHSA-2020:4760
https://access.redhat.com/errata/RHSA-2020:4763
https://access.redhat.com/errata/RHSA-2020:4766
https://access.redhat.com/errata/RHSA-2020:4799
https://access.redhat.com/errata/RHSA-2020:4805
https://access.redhat.com/errata/RHSA-2020:4806
https://access.redhat.com/errata/RHSA-2020:4807
https://access.redhat.com/errata/RHSA-2020:4820
https://access.redhat.com/errata/RHSA-2020:4827
https://access.redhat.com/errata/RHSA-2020:4844
https://access.redhat.com/errata/RHSA-2020:4846
https://access.redhat.com/errata/RHSA-2020:4847
https://access.redhat.com/errata/RHSA-2020:4900
https://access.redhat.com/errata/RHSA-2020:4903
https://access.redhat.com/errata/RHSA-2020:4907
https://access.redhat.com/errata/RHSA-2020:4908
https://access.redhat.com/errata/RHSA-2020:4910
https://access.redhat.com/errata/RHSA-2020:4922
https://access.redhat.com/errata/RHSA-2020:4923
https://access.redhat.com/errata/RHSA-2020:4929
https://access.redhat.com/errata/RHSA-2020:4930
https://access.redhat.com/errata/RHSA-2020:4931
https://access.redhat.com/errata/RHSA-2020:4932
https://access.redhat.com/errata/RHSA-2020:4946
https://access.redhat.com/errata/RHSA-2020:4949
https://access.redhat.com/errata/RHSA-2020:4950
https://access.redhat.com/errata/RHSA-2020:4951
https://access.redhat.com/errata/RHSA-2020:4952
https://access.redhat.com/errata/RHSA-2020:4953
https://access.redhat.com/errata/RHSA-2020:4960
https://access.redhat.com/errata/RHSA-2020:4961

17. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20203107-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203115-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203121-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203122-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203125-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203126-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203132-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203133-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203143-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203147-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203149-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203151-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203152-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203155-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203159-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203160-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203161-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203162-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203163-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203164-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203165-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203166-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203171-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203178-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203180-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203181-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203186-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203187-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203188-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203190-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203191-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014524-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014525-1/

18. Trend Micro InterScan Messaging Virtual Appliance

https://success.trendmicro.com/solution/000279833

19. Ubuntu

https://ubuntu.com/security/notices/USN-4599-3
https://ubuntu.com/security/notices/USN-4605-2
https://ubuntu.com/security/notices/USN-4611-1
https://ubuntu.com/security/notices/USN-4613-1
https://ubuntu.com/security/notices/USN-4614-1
https://ubuntu.com/security/notices/USN-4615-1
https://ubuntu.com/security/notices/USN-4616-1
https://ubuntu.com/security/notices/USN-4616-2
https://ubuntu.com/security/notices/USN-4617-1
https://ubuntu.com/security/notices/USN-4618-1
https://ubuntu.com/security/notices/USN-4619-1

https://ubuntu.com/security/notices/USN-4620-1

20. WAGO Series 750-88x and 750-352

https://us-cert.cisa.gov/ics/advisories/icsa-20-308-01

21. WECON PLC Editor

https://us-cert.cisa.gov/ics/advisories/icsa-20-310-01

Sources of product vulnerability information:

Android
Apple
Cisco
Debian
F5
Fortinet
Gentoo Linux
Google Chrome
Huawei
openSUSE
Oracle Linux
QNAP
Red Hat
SUSE
Trend Micro
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk