GovCERT.HK

Weekly IT Security News Bulletin, 2020-W22

25 May – 31 May 2020

Headlines

RangeAmp attacks on websites and CDN servers

- The Hyper Text Transfer Protocol (HTTP) Range request is a kind of web requests to get partial resource content from web servers, facilitating suspension and resumption of traffic during large media or file downloads. A content delivery network (CDN) is an Internet infrastructure deployed to offload response of web requests from web servers to geographically distributed cache servers so as to enhance service performance and scalability as well as to protect web servers against distributed denial-of-service (DDoS) attacks.

- A team of academic researchers found that a little malformed HTTP Range requests delivered to CDNs could trigger a large volume of traffic against the CDN servers and the web servers behind, actualising a denial-of-service (DoS) attack. Such attack method is known as RangeAmp which has two variants: Small Byte Range (SBR) and Overlapping Byte Range (OBR). The SBR attack could exploit CDN servers to amplify the attack traffic targeting on the actual web server. The OBR attack could cause traffic amplification among CDN servers within the provider's network thus disrupting the CDN service in addition to leaving the actual web server inaccessible.

- The SBR attack traffic could be multiplied from 724 to 43,330 times and the OBR attack traffic could also be boosted up to 7,500 times. The researchers tested the attacks on 13 various CDN providers' networks. All of them were found to be vulnerable to the SBR attack while six of them were susceptible to the OBR attack as well. The researchers reported that 12 affected CDN providers had either fixed the vulnerability in their HTTP Range request implementation or got plans to do so.

Advice

- CDN providers should fix their HTTP Range request implementation vulnerability.

- CDN consumers could consult their CDN providers for whether their services are affected by the RangeAmp vulnerabilities.

- Organisations may subscribe redundant CDN services from different providers for higher resilience.

Sources

- Baojun Liu
- ZDNet

2020 DevSecOps Survey

- DevSecOps is an approach to integrate development, security, and operations in software implementation. A project management platform vendor conducted its Global DevSecOps Survey in February 2020 collecting views of almost 3,700 software development practitioners from 21 countries. The survey reflected shifting roles between developers, security teams, operations teams and testers.

- More than 34% of developers took up the operational responsibilities in setting up the healthy infrastructure for running applications. Around 28% of developers told that they were devoted to security tasks in their organisations. On the other hand, 65% of security teams reported that security was brought earlier into the development cycle while they became part of cross-functional teams and worked more closely with developers.

- Testing was regarded by 47% of respondents as the top reason of project delays. Shadowed by the trouble with testing, nearly 75% of organisations would take testing earlier in the development life cycle. More developers would carry out testing and more automated testing would be involved. In 17% of organisations, development and testing teams would work together when code is being written.

Advice

- Security implementation should be brought into the software development process from the outset.

- Security testing should be included into the project plan as an essential component as functional testing.

- Security training should be provided to all development, operations, and testing team members for fostering application security best practices among them and facilitating their closer collaboration with security teams.

Sources

- GitLab
- IT Brief

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/en-us/HT211170
https://support.apple.com/en-us/HT211177
https://support.apple.com/en-us/HT211178
https://support.apple.com/en-us/HT211179
https://support.apple.com/en-us/HT211181
https://support.apple.com/en-us/HT211186

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-salt-2vx545AG

3. Debian

https://www.debian.org/security/2020/dsa-4691
https://www.debian.org/security/2020/dsa-4692
https://www.debian.org/security/2020/dsa-4693
https://www.debian.org/security/2020/dsa-4694

4. F5 Products

https://support.f5.com/csp/article/K05544642
https://support.f5.com/csp/article/K97810133

5. Fortinet FortiClient

https://fortiguard.com/psirt/FG-IR-20-040

6. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200527-01-dos-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200527-01-wifi-en

7. Inductive Automation Ignition

https://www.us-cert.gov/ics/advisories/icsa-20-147-01

8. Johnson Controls Kantech EntraPass

https://www.us-cert.gov/ics/advisories/icsa-20-147-02

9. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00039.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00040.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00041.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00042.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00043.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00044.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00045.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00046.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00047.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00048.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00049.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00050.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00051.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00052.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00053.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00054.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00055.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00056.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00057.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00058.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00059.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00060.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00061.html
https://lists.opensuse.org/opensuse-security-announce/2020-05/msg00062.html

10. Red Hat

https://access.redhat.com/errata/RHSA-2020:2217
https://access.redhat.com/errata/RHSA-2020:2218
https://access.redhat.com/errata/RHSA-2020:2263
https://access.redhat.com/errata/RHSA-2020:2265
https://access.redhat.com/errata/RHSA-2020:2274
https://access.redhat.com/errata/RHSA-2020:2276
https://access.redhat.com/errata/RHSA-2020:2277
https://access.redhat.com/errata/RHSA-2020:2284
https://access.redhat.com/errata/RHSA-2020:2285
https://access.redhat.com/errata/RHSA-2020:2286
https://access.redhat.com/errata/RHSA-2020:2289
https://access.redhat.com/errata/RHSA-2020:2291
https://access.redhat.com/errata/RHSA-2020:2295
https://access.redhat.com/errata/RHSA-2020:2296
https://access.redhat.com/errata/RHSA-2020:2297
https://access.redhat.com/errata/RHSA-2020:2298
https://access.redhat.com/errata/RHSA-2020:2320
https://access.redhat.com/errata/RHSA-2020:2321
https://access.redhat.com/errata/RHSA-2020:2333
https://access.redhat.com/errata/RHSA-2020:2334
https://access.redhat.com/errata/RHSA-2020:2335
https://access.redhat.com/errata/RHSA-2020:2336
https://access.redhat.com/errata/RHSA-2020:2337
https://access.redhat.com/errata/RHSA-2020:2338

11. Symantec Products

https://support.broadcom.com/security-advisory/security-advisory-detail.html?notificationId=SYMSA1768

12. Ubuntu

https://usn.ubuntu.com/4359-2/
https://usn.ubuntu.com/4360-4/
https://usn.ubuntu.com/4363-1/
https://usn.ubuntu.com/4367-2/
https://usn.ubuntu.com/4369-2/
https://usn.ubuntu.com/4374-1/
https://usn.ubuntu.com/4375-1/
https://usn.ubuntu.com/4376-1/

Sources of product vulnerability information:

Apple
Broadcom
Cisco
Debian
F5
Fortiguard
Huawei
openSUSE
Red Hat
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk