GovCERT.HK

Weekly IT Security News Bulletin, 2020-W44

26 October – 1 November 2020

Headlines

WebLogic servers under attack

- WebLogic server, a Java Enterprise Edition (J2EE) application server developed by Oracle, suffers from a severe vulnerability and now comes under attack in the wild.
- This vulnerability in WebLogic servers was first revealed in Oracle's critical patch update released in mid-October. The vulnerability can be exploited remotely via network access to compromise the servers.
- Within a week after the patch was released, a researcher developed a proof-of-concept (PoC) and published it in his blog. The PoC shows that an attacker can compromise vulnerable WebLogic servers by simply sending a specially crafted HTTP GET request to the servers.
- According to SANS Internet Storm Center, active exploitation of the vulnerability against their honeypot was observed after the PoC had been released. While those attempts mainly aimed to verify whether the target systems were vulnerable, a security vendor found a number of Internet-facing WebLogic servers were not patched and vulnerable to attacks. It is believed that more attacks will follow.

Advice

- Deploy the patch immediately on the affected servers.
- Block access of admin portal from the Internet where possible.
- Monitor network traffic for any suspicious HTTP requests and processes.

Sources

- Rapid7
- HelpNetSecurity
- Jang's Blog (in Vietnamese)

Ransomware attack on coffee makers

- Security of Internet of things (IoT) devices is always ignored by manufacturers and users and has become one of the weakest links in cyber security. Recently, a security researcher demonstrated how a network-connected coffee maker can be turned into a ransomware machine by injecting malicious code through firmware update.

- Given that firmware has no encryption or protection and its update is carried out through unencrypted network, attackers can spoof legitimate update and remotely replace the device's firmware. Besides ransomware attack, the infected devices can potentially be used for other malicious purposes like denial of service, sniffing, data theft, etc.

- Actually, IoT devices can be of different forms, from coffee makers and refrigerators to physical systems and environmental controls. They can be a stepping stone for attackers to get a foothold in private networks and infect other machines in it.

- The researcher also pointed out that given the long lifespan of IoT devices like refrigerators or home appliances, manufacturers of the devices may only be willing to provide technical support including security or firmware updates for the devices for a short period of time. Those unsupported IoT devices can become vulnerable and be exploited by attackers.

Advice

- Adopt network segmentation and avoid connecting untrusted devices to sub-networks with sensitive data or systems.
- Apply latest firmware and security patches on devices and stop using unsupported devices.
- Check the legitimacy of firmware and verify its digital signature if signed.

Sources

- DarkReading
- MalwareByteLabs
- Avast

Product Vulnerability Notes & Security Updates

1. Citrix Hypervisor

https://support.citrix.com/article/CTX284874

2. Debian

https://www.debian.org/security/2020/dsa-4779
https://www.debian.org/security/2020/dsa-4781

3. F5 Products

https://support.f5.com/csp/article/K12002065
https://support.f5.com/csp/article/K23278332
https://support.f5.com/csp/article/K25400442
https://support.f5.com/csp/article/K26244025
https://support.f5.com/csp/article/K38157961
https://support.f5.com/csp/article/K44020030
https://support.f5.com/csp/article/K44808538
https://support.f5.com/csp/article/K55053009
https://support.f5.com/csp/article/K58290051
https://support.f5.com/csp/article/K62830532
https://support.f5.com/csp/article/K76610106

4. Gentoo Linux

https://security.gentoo.org/glsa/202010-07
https://security.gentoo.org/glsa/202010-08

5. IBM WebSphere Application Server

https://www.ibm.com/support/pages/node/6356083

6. Mitsubishi Electric Products

https://us-cert.cisa.gov/ics/advisories/icsa-20-303-01
https://us-cert.cisa.gov/ics/advisories/icsa-20-303-02

7. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00048.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00049.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00050.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00051.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00052.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00053.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00054.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00055.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00056.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00057.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00058.html

https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00059.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00060.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00061.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00062.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00063.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00064.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00065.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00066.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00067.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00068.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00069.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00070.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00071.html

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-4276.html
https://linux.oracle.com/errata/ELSA-2020-4307.html
https://linux.oracle.com/errata/ELSA-2020-4310.html
https://linux.oracle.com/errata/ELSA-2020-4317.html
https://linux.oracle.com/errata/ELSA-2020-4347.html
https://linux.oracle.com/errata/ELSA-2020-4348.html
https://linux.oracle.com/errata/ELSA-2020-4350.html
https://linux.oracle.com/errata/ELSA-2020-5900.html

9. QNAP Products

https://www.qnap.com/en/security-advisory/qsa-20-09

10. Red Hat

https://access.redhat.com/errata/RHSA-2020:4283
https://access.redhat.com/errata/RHSA-2020:4297
https://access.redhat.com/errata/RHSA-2020:4298
https://access.redhat.com/errata/RHSA-2020:4320
https://access.redhat.com/errata/RHSA-2020:4330
https://access.redhat.com/errata/RHSA-2020:4331
https://access.redhat.com/errata/RHSA-2020:4332
https://access.redhat.com/errata/RHSA-2020:4344
https://access.redhat.com/errata/RHSA-2020:4347
https://access.redhat.com/errata/RHSA-2020:4348
https://access.redhat.com/errata/RHSA-2020:4349
https://access.redhat.com/errata/RHSA-2020:4350
https://access.redhat.com/errata/RHSA-2020:4351
https://access.redhat.com/errata/RHSA-2020:4352
https://access.redhat.com/errata/RHSA-2020:4366
https://access.redhat.com/errata/RHSA-2020:4381
https://access.redhat.com/errata/RHSA-2020:4383
https://access.redhat.com/errata/RHSA-2020:4384
https://access.redhat.com/errata/RHSA-2020:4390
https://access.redhat.com/errata/RHSA-2020:4391
https://access.redhat.com/errata/RHSA-2020:4401
https://access.redhat.com/errata/RHSA-2020:4402

11. SHUN HU Technology JUUKO Industrial Radio Remote Control

https://us-cert.cisa.gov/ics/advisories/icsa-20-301-01

12. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20201396-3/
https://www.suse.com/support/update/announcement/2020/suse-su-20203014-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203016-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203021-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203022-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203023-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203024-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203030-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203034-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203036-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203037-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203038-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203039-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203045-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203049-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203050-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203051-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203052-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203053-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203054-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203060-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203064-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203065-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203067-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203068-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203069-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203070-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203071-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203073-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203080-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203081-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203082-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203083-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203084-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203085-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203086-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203087-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203088-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203089-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203090-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203091-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203092-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203093-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203094-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203095-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203096-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014522-1/

13. Ubuntu

https://ubuntu.com/security/notices/USN-3081-2
https://ubuntu.com/security/notices/USN-4552-3
https://ubuntu.com/security/notices/USN-4562-2
https://ubuntu.com/security/notices/USN-4583-2
https://ubuntu.com/security/notices/USN-4599-1
https://ubuntu.com/security/notices/USN-4599-2
https://ubuntu.com/security/notices/USN-4600-2
https://ubuntu.com/security/notices/USN-4602-1
https://ubuntu.com/security/notices/USN-4602-2
https://ubuntu.com/security/notices/USN-4603-1
https://ubuntu.com/security/notices/USN-4604-1
https://ubuntu.com/security/notices/USN-4605-1
https://ubuntu.com/security/notices/USN-4607-1
https://ubuntu.com/security/notices/USN-4608-1
https://ubuntu.com/security/notices/USN-4609-1
https://ubuntu.com/security/notices/USN-4610-1

14. VMware

https://www.vmware.com/security/advisories/VMSA-2020-0024.html

15. Wireshark

https://www.wireshark.org/security/wnpa-sec-2020-14.html
https://www.wireshark.org/security/wnpa-sec-2020-15.html

16. WordPress

https://wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance-release/

Sources of product vulnerability information:

Citrix
Debian
F5
Gentoo Linux
IBM
openSUSE
Oracle Linux
QNAP
Red Hat
SUSE
Ubuntu
US-CERT
VMware
Wireshark
WordPress

Contact:

cert@govcert.gov.hk