GovCERT.HK

Weekly IT Security News Bulletin, 2017-W37

11 September – 17 September 2017

Headlines

BlueBorne: a new attack vector comes to Bluetooth devices

- BlueBorne, a collection of 8 Bluetooth implementation vulnerabilities, potentially puts billions of devices with Bluetooth capability at the risk of being compromised. The vulnerabilities affect almost all major mobile and computer operating systems, including Microsoft Windows, Linux, Apple iOS and Android. With BlueBorne flaws, attackers can access sensitive information, execute arbitrary code on the devices or even take complete control over the targeted devices, through Bluetooth connections but without pairing in advance.

- The BlueBorne vulnerabilities can bring devastating effect. Firstly, attacks can spread over the air without any user interactions involved and prior configuration required. Secondly, unlike most attacks today, exploiting the vulnerabilities requires only an active Bluetooth connection but not Internet access. It provides an opportunity for attackers to penetrate into secure internal networks even though they are isolated. Lastly, attacks against the vulnerabilities can bypass the traditional security measures put in place in the devices, making them undetectable.

- Although some of the product vendors have released patches for the vulnerabilities, researchers estimated that 40% of all Bluetooth-enabled devices may not receive patches because of the products reaching end-of-life or not being supported.

Advice

- Update the operating systems of Bluetooth-enabled devices to the latest version.

- Disable the Bluetooth function or minimising its use if it is unused or unnecessary, in particular for those affected products without patches released.

- Plan for replacing end-of life devices to avoid the security risk of using de-supported hardware.

Sources

- Armis
- Threatpost
- Bleeping Computer
- The Hacker News

Upgrade Apache Struts immediately to fix another actively exploiting flaw

- The popular, open-source Apache Struts development framework was threatened by another critical vulnerability identified as CVE-2017-9805. The vulnerability affects servers running web applications that are built upon Apache Struts versions 2.1.2 through 2.3.33 and 2.5 through 2.5.12, as well as using associated REST plugin. The flaw may also resides in some off-the-shelf computer devices or systems, including portion of Cisco products.

- Remote and unprivileged attacker can take advantage of this particular vulnerability to execute arbitrary code in the context of vulnerable Struts applications. According to the analysis made by security researchers, the weaknesses were caused by the failure of Apache Struts to filter untrusted XML data when processing a HTTP request carrying specially crafted and malicious XML payload.

- To fix the flaw, the Apache Software Foundation released Struts 2.3.34 and 2.5.13. There is no specific workaround available at the moment and upgrading of Apache Struts is the only way to fix the vulnerability. It is worth noting that a proof-of-concept but fully workable exploit code has been made publicly available on the Internet and active exploitation targeting the vulnerability was also observed.

Advice

- Upgrade Apache Struts in your web applications to the latest version or remove the REST plugin if it is unnecessary.

- Check with product vendors to confirm if the systems are affected and the availability of patches and if so, upgrade to the fixed version.

- Closely monitor any suspicious activities before the upgrade is applied.

Sources

- Bleeping Computer
- Security Week
- The Register
- SC Magazine
- lgtm

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player**
   https://helpx.adobe.com/security/products/flash-player/apsb17-28.html
   https://www.hkcert.org/my_url/en/alert/17091302

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-September/022530.html
   https://lists.centos.org/pipermail/centos-announce/2017-September/022531.html
   https://lists.centos.org/pipermail/centos-announce/2017-September/022535.html
   https://lists.centos.org/pipermail/centos-announce/2017-September/022536.html
   https://lists.centos.org/pipermail/centos-announce/2017-September/022540.html

3. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170909-struts2-rce

4. **Debian**
   https://www.debian.org/security/2017/dsa-3967
   https://www.debian.org/security/2017/dsa-3968
   https://www.debian.org/security/2017/dsa-3969
   https://www.debian.org/security/2017/dsa-3970
   https://www.debian.org/security/2017/dsa-3971
   https://www.debian.org/security/2017/dsa-3972

5. **F5 Products**
   https://support.f5.com/csp/article/K11220361

6. **LOYTEC LVIS-3ME**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-257-01

7. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0334.html
   http://advisories.mageia.org/MGASA-2017-0335.html
   http://advisories.mageia.org/MGASA-2017-0336.html
   http://advisories.mageia.org/MGASA-2017-0337.html
   http://advisories.mageia.org/MGASA-2017-0338.html
   http://advisories.mageia.org/MGASA-2017-0339.html

8. **Microsoft**
   https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/5984735e-f651-e711-80dd-000d3a32fc99
   https://support.microsoft.com/en-us/help/20170912/security-update-deployment-information-september-12-2017
   https://www.hkcert.org/my_url/en/alert/17091301

9. **mySCADA myPRO**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-255-01

10. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00019.html
    https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00020.html

https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00021.html
https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00022.html
https://lists.opensuse.org/opensuse-security-announce/2017-09/msg00023.html

11. Oracle Linux

https://linux.oracle.com/errata/ELSA-2017-2412.html
https://linux.oracle.com/errata/ELSA-2017-2679.html
https://linux.oracle.com/errata/ELSA-2017-2679-1.html
https://linux.oracle.com/errata/ELSA-2017-2681.html
https://linux.oracle.com/errata/ELSA-2017-2685.html
https://linux.oracle.com/errata/ELSA-2017-2728.html

12. Red Hat

https://access.redhat.com/errata/RHSA-2017:2676
https://access.redhat.com/errata/RHSA-2017:2677
https://access.redhat.com/errata/RHSA-2017:2678
https://access.redhat.com/errata/RHSA-2017:2679
https://access.redhat.com/errata/RHSA-2017:2680
https://access.redhat.com/errata/RHSA-2017:2681
https://access.redhat.com/errata/RHSA-2017:2682
https://access.redhat.com/errata/RHSA-2017:2683
https://access.redhat.com/errata/RHSA-2017:2685
https://access.redhat.com/errata/RHSA-2017:2687
https://access.redhat.com/errata/RHSA-2017:2692
https://access.redhat.com/errata/RHSA-2017:2693
https://access.redhat.com/errata/RHSA-2017:2698
https://access.redhat.com/errata/RHSA-2017:2702
https://access.redhat.com/errata/RHSA-2017:2704
https://access.redhat.com/errata/RHSA-2017:2705
https://access.redhat.com/errata/RHSA-2017:2706
https://access.redhat.com/errata/RHSA-2017:2707
https://access.redhat.com/errata/RHSA-2017:2708
https://access.redhat.com/errata/RHSA-2017:2709
https://access.redhat.com/errata/RHSA-2017:2710
https://access.redhat.com/errata/RHSA-2017:2726
https://access.redhat.com/errata/RHSA-2017:2727
https://access.redhat.com/errata/RHSA-2017:2728
https://access.redhat.com/errata/RHSA-2017:2731
https://access.redhat.com/errata/RHSA-2017:2732

13. Slackware

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.336363
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.353960
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.503015
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.545149
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.928329

14. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20172389-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172390-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172416-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172419-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172420-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172422-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172423-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172424-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172436-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172437-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172438-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172439-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172440-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172441-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20172442-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172443-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172446-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172447-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172448-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172449-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172450-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172453-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172454-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172455-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172456-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172457-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172458-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172459-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172464-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172465-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172466-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172467-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172468-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172469-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172470-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172471-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172472-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172473-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172474-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172475-1/
https://www.suse.com/support/update/announcement/2017/suse-su-20172476-1/

15. **Ubuntu**

https://usn.ubuntu.com/usn/usn-3413-1/
https://usn.ubuntu.com/usn/usn-3414-1/
https://usn.ubuntu.com/usn/usn-3415-1/
https://usn.ubuntu.com/usn/usn-3415-2/
https://usn.ubuntu.com/usn/usn-3416-1/
https://usn.ubuntu.com/usn/usn-3417-1/

16. **Xen**

http://xenbits.xen.org/xsa/advisory-231.html

http://xenbits.xen.org/xsa/advisory-232.html
http://xenbits.xen.org/xsa/advisory-233.html
http://xenbits.xen.org/xsa/advisory-234.html

Sources of product vulnerability information:

Adobe
CentOS
Cisco
Debian
F5
HKCERT
ICS-CERT
Mageia
Microsoft
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
Xen

Contacts:

cert@govcert.gov.hk