GovCERT.HK

Weekly IT Security News Bulletin, 2020-W34
17 August – 23 August 2020

Headlines

Digitally signed Windows files being spoofed by GlueBall

- GlueBall is a vulnerability on Windows operating systems, allowing an attacker to evade detection of digitally signed files that have been tampered. It is also referenced as CVE-2020-1464 and has been fixed in Microsoft's August 2020 Patch Tuesday updates.

- Digital signatures are used by Windows operating systems to validate that files being downloaded onto the systems come from trustable sources. The GlueBall bug appears at the system function used to validate the contents of Microsoft Installer (MSI) files. The function just examines the beginning of an MSI file for verification and signature validation but neglects the remaining part of the file.

- An attacker could append a malicious Java program to a digitally signed MSI file such that a vulnerable system would still recognise the contaminated file as a valid one from a trusted source. Since the Java program would be parsed from the end of the file for execution neglecting the precedent part of the file, such exploitation is particularly effective to match the faulty signature verification process, which only checks the former part of the file.

Advice

- Update your Windows systems to fix the GlueBall vulnerability.

- Download and install programs only from official websites.

- Check cryptographic checksums of downloaded programs if available, in addition to validating digital signatures, as an extra security measure.

Sources

- Medium
- SecurityWeek

Duri: An HTML smuggling campaign

- HTML smuggling is a technique adopted by attackers to distribute malicious files or programs to web client devices stealthily. A web isolation solution vendor discovered an ongoing HTML smuggling campaign which began in early July 2020. The attack campaign is named "Duri".

- In the Duri attack, the malicious file does not come directly from a universal resource locator (URL). When users click on the URL provided by the attacker, they are redirected multiple times and finally led to a landing web page of the domain "duckdns[.]org". The web browser is triggered to run the JavaScript loaded together with the web page. It is the JavaScript code that constructs the malicious file from encoded data on the spot within the browser.

- The locally generated malicious file is a ZIP archive containing a Microsoft Windows Installer (MSI) file, which is embedded with an obfuscated JScript program to carry out further operations. Since the malicious ZIP file is not distributed through the network, the smuggling method bypasses any network-based security checking at proxies, firewalls and sandboxes for protecting web clients.

Advice

- Deploy endpoint detection and response solutions in addition to network-based security solutions to form a multiple layer of defence against various attacks.

- Do not grant administrative privileges to end user accounts to minimise impacts of attacks through end user applications such as web browsers.

- Educate end users not to click URLs from unsolicited emails or other unknown sources.

- Consider to deploy web isolation solutions which could prevent any malicious JavaScript from running at end users' computers.

Sources

- Menlo Security
- BleepingComputer

Product Vulnerability Notes & Security Updates

1. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cdp-memleak-k5Z7m55t
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmx-prvesc-6g37hjAL
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmx-rshell-esc-L6hBwjbg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvdsd-pathtrv-5tLJRrFn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvdsd-rbac-y9LM5jw4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvdsd-xss-teMmLyUr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-auth-bypass-MYeFpFcF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-authbypass-YVJzqgk2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-bypass-auth-mVDR6ygT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-file-path-6PKONjHe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-infordisc-DOAXVvFV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-pa-trav-bMdfSTTq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-patrav-pW9RkhyW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-5TdMJRB3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-JnHSWG5C
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-stored-w4rJZJtO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-mlt-xss-zUzbcdEV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-HYP-WSV-yT3j5hSB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcameras-rce-dos-uPyJYxN3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbss-ipv6-dos-tsgqbffW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smart-priv-esca-nqwxXWBu
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vdsd-W7mnkwj7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-encsw-cspw-cred-hZzL29A7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-desktop-app-OVSfpVMj

2. Debian

https://www.debian.org/security/2020/dsa-4746

3. Gentoo Linux

https://security.gentoo.org/glsa/202008-08

4. Google Chrome

https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_18.html

5. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00031.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00033.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00034.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00035.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00036.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00037.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00038.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00039.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00040.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00041.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00042.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00043.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00044.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00045.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00046.html

6. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-3422.html

7. Red Hat

https://access.redhat.com/errata/RHSA-2020:3453
https://access.redhat.com/errata/RHSA-2020:3456
https://access.redhat.com/errata/RHSA-2020:3461
https://access.redhat.com/errata/RHSA-2020:3462
https://access.redhat.com/errata/RHSA-2020:3463
https://access.redhat.com/errata/RHSA-2020:3464
https://access.redhat.com/errata/RHSA-2020:3470
https://access.redhat.com/errata/RHSA-2020:3471
https://access.redhat.com/errata/RHSA-2020:3475
https://access.redhat.com/errata/RHSA-2020:3495
https://access.redhat.com/errata/RHSA-2020:3496
https://access.redhat.com/errata/RHSA-2020:3497
https://access.redhat.com/errata/RHSA-2020:3501
https://access.redhat.com/errata/RHSA-2020:3504
https://access.redhat.com/errata/RHSA-2020:3505
https://access.redhat.com/errata/RHSA-2020:3518
https://access.redhat.com/errata/RHSA-2020:3525

8. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.417972

9. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20202237-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202238-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202251-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202258-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202259-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202264-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202265-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202266-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202267-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202269-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202271-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202272-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202274-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202275-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202276-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202277-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202283-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014454-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014456-1/

10. Treck TCP/IP Stack

https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

11. Trend Micro Products

https://success.trendmicro.com/solution/000252039

12. Ubuntu

https://ubuntu.com/security/notices/USN-4456-2
https://ubuntu.com/security/notices/USN-4457-2
https://ubuntu.com/security/notices/USN-4459-1
https://ubuntu.com/security/notices/USN-4460-1
https://ubuntu.com/security/notices/USN-4461-1
https://ubuntu.com/security/notices/USN-4462-1
https://ubuntu.com/security/notices/USN-4463-1
https://ubuntu.com/security/notices/USN-4464-1
https://ubuntu.com/security/notices/USN-4465-1
https://ubuntu.com/security/notices/USN-4466-1
https://ubuntu.com/security/notices/USN-4466-2
https://ubuntu.com/security/notices/USN-4467-1

Sources of product vulnerability information:

Cisco
Debian
Gentoo Linux
Google Chrome
openSUSE
Oracle Linux

Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk