GovCERT.HK

Weekly IT Security News Bulletin, 2020-W51

14 December – 20 December 2020

Headlines

Supply chain attack threatening organisations around the world

- A security vendor who fell victim in a system breach earlier this month discovered that SolarWinds Orion, an IT monitoring and management solution, was compromised to deliver malware.
- Malicious actors compromised the software build system of Orion and injected a backdoor called "SUNBURST" into the software build, which was then delivered via software update released between March and June 2020 to Orion users.
- SUNBURST once loaded will try to connect to the command and control server for instructions. It can perform various malicious tasks on infected device like exfiltrate data, retrieve and run code or other malware, erase or tamper with files, etc. Those target victims can be subject to follow-on action and further infection ((e.g., Teardrop and a Cobalt Strike) by the malicious actors.
- About 18,000 Orion customers using the infected version of the software could be impacted by the attack and were urged to apply the latest update (version 2020.2.1 HF 2) or disconnect the affected devices as soon as possible. The affected customers include organisations in various countries and from various sectors including government, telecommunication and technology.

Advice

- Apply the latest updates on the affected software.
- Developers should perform regular inspection on their codebase and check for any signs of tampering or malicious code.
- Identify the applications and software used in your environment and review their security risk levels.
- Monitor network traffic and review system logs for suspicious activities.

Sources

- CISA
- FireEye
- The Hacker News
- Bleeping Computer

Vulnerable WordPress plugin allows unrestricted file upload

- A researcher recently found a critical vulnerability in a popular WordPress plugin called "Contact Form 7" which is used in millions of WordPress instances for creating and managing contact forms.

- The vulnerability allows attackers to upload arbitrary files containing malicious code to WordPress sites with the affected version of the plugin and execute the file as scripts on the servers. This can potentially result in injection of malicious content, defacement or even taking over of the website.

- The vulnerability can be attributed to the flaw of double extension in the filename sanitisation process of the plugin and similar issue was previously found in Drupal in November 2020. The plugin fails to properly handle filenames with two extensions separated by a special character and can only preserve the filename string up to the first extension, discarding the latter extension after the separator. The extension of the file will therefore be changed arbitrarily by manipulating the filename.

- An update of the plugin was released on 17 December to fix the vulnerability.

Advice

- Avoid or minimise the use of plugins to reduce security risks.
- Apply updates and patches to the plugins in a timely manner.
- Validate and sanitise input or file uploaded by users.

Sources

- Astra
- Threatpost
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/zh-tw/HT211932
https://support.apple.com/zh-tw/HT212007
https://support.apple.com/zh-tw/HT212011

2. CentOS

https://lists.centos.org/pipermail/centos-announce/2020-December/048211.html
https://lists.centos.org/pipermail/centos-announce/2020-December/048217.html
https://lists.centos.org/pipermail/centos-announce/2020-December/048218.html
https://lists.centos.org/pipermail/centos-announce/2020-December/048222.html
https://lists.centos.org/pipermail/centos-announce/2020-December/048224.html
https://lists.centos.org/pipermail/centos-announce/2020-December/048237.html

3. Citrix Hypervisor

https://support.citrix.com/article/CTX286756

4. Debian

https://www.debian.org/security/2020/dsa-4810
https://www.debian.org/security/2020/dsa-4811
https://www.debian.org/security/2020/dsa-4812
https://www.debian.org/security/2020/dsa-4813
https://www.debian.org/security/2020/dsa-4814

5. Emerson Rosemount X-STREAM

https://us-cert.cisa.gov/ics/advisories/icsa-20-352-01

6. F5 Products

https://support.f5.com/csp/article/K01869532
https://support.f5.com/csp/article/K04048104
https://support.f5.com/csp/article/K04518313
https://support.f5.com/csp/article/K09081535
https://support.f5.com/csp/article/K15310332
https://support.f5.com/csp/article/K19166530
https://support.f5.com/csp/article/K21404407
https://support.f5.com/csp/article/K25595031
https://support.f5.com/csp/article/K25691186
https://support.f5.com/csp/article/K30343902
https://support.f5.com/csp/article/K41301038
https://support.f5.com/csp/article/K42933418
https://support.f5.com/csp/article/K43850230
https://support.f5.com/csp/article/K45143221
https://support.f5.com/csp/article/K50343630
https://support.f5.com/csp/article/K51574311
https://support.f5.com/csp/article/K52035247

https://support.f5.com/csp/article/K58102101
https://support.f5.com/csp/article/K60344652
https://support.f5.com/csp/article/K73657294

7. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en

8. IBM WebSphere Application Server

https://www.ibm.com/support/pages/node/6381362
https://www.ibm.com/support/pages/node/6382238

9. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-5393.html
https://linux.oracle.com/errata/ELSA-2020-5401.html
https://linux.oracle.com/errata/ELSA-2020-5402.html
https://linux.oracle.com/errata/ELSA-2020-5408.html
https://linux.oracle.com/errata/ELSA-2020-5434.html
https://linux.oracle.com/errata/ELSA-2020-5435.html
https://linux.oracle.com/errata/ELSA-2020-5437.html
https://linux.oracle.com/errata/ELSA-2020-5439.html
https://linux.oracle.com/errata/ELSA-2020-5443.html
https://linux.oracle.com/errata/ELSA-2020-5473.html
https://linux.oracle.com/errata/ELSA-2020-5476.html
https://linux.oracle.com/errata/ELSA-2020-5480.html
https://linux.oracle.com/errata/ELSA-2020-5495.html
https://linux.oracle.com/errata/ELSA-2020-5499.html
https://linux.oracle.com/errata/ELSA-2020-5500.html
https://linux.oracle.com/errata/ELSA-2020-5561-1.html
https://linux.oracle.com/errata/ELSA-2020-5562-1.html
https://linux.oracle.com/errata/ELSA-2020-5566-1.html
https://linux.oracle.com/errata/ELSA-2020-5607-1.html
https://linux.oracle.com/errata/ELSA-2020-5995.html
https://linux.oracle.com/errata/ELSA-2020-5996.html

10. PTC Kepware Products

https://us-cert.cisa.gov/ics/advisories/icsa-20-352-02
https://us-cert.cisa.gov/ics/advisories/icsa-20-352-03

11. Red Hat

https://access.redhat.com/errata/RHSA-2020:5259
https://access.redhat.com/errata/RHSA-2020:5260
https://access.redhat.com/errata/RHSA-2020:5359
https://access.redhat.com/errata/RHSA-2020:5361
https://access.redhat.com/errata/RHSA-2020:5363
https://access.redhat.com/errata/RHSA-2020:5393
https://access.redhat.com/errata/RHSA-2020:5394
https://access.redhat.com/errata/RHSA-2020:5395

https://access.redhat.com/errata/RHSA-2020:5396
https://access.redhat.com/errata/RHSA-2020:5401
https://access.redhat.com/errata/RHSA-2020:5402
https://access.redhat.com/errata/RHSA-2020:5408
https://access.redhat.com/errata/RHSA-2020:5410
https://access.redhat.com/errata/RHSA-2020:5411
https://access.redhat.com/errata/RHSA-2020:5412
https://access.redhat.com/errata/RHSA-2020:5416
https://access.redhat.com/errata/RHSA-2020:5417
https://access.redhat.com/errata/RHSA-2020:5418
https://access.redhat.com/errata/RHSA-2020:5420
https://access.redhat.com/errata/RHSA-2020:5422
https://access.redhat.com/errata/RHSA-2020:5423
https://access.redhat.com/errata/RHSA-2020:5428
https://access.redhat.com/errata/RHSA-2020:5430
https://access.redhat.com/errata/RHSA-2020:5434
https://access.redhat.com/errata/RHSA-2020:5435
https://access.redhat.com/errata/RHSA-2020:5437
https://access.redhat.com/errata/RHSA-2020:5439
https://access.redhat.com/errata/RHSA-2020:5441
https://access.redhat.com/errata/RHSA-2020:5443
https://access.redhat.com/errata/RHSA-2020:5453
https://access.redhat.com/errata/RHSA-2020:5473
https://access.redhat.com/errata/RHSA-2020:5476
https://access.redhat.com/errata/RHSA-2020:5479
https://access.redhat.com/errata/RHSA-2020:5480
https://access.redhat.com/errata/RHSA-2020:5483
https://access.redhat.com/errata/RHSA-2020:5487
https://access.redhat.com/errata/RHSA-2020:5493
https://access.redhat.com/errata/RHSA-2020:5495
https://access.redhat.com/errata/RHSA-2020:5499
https://access.redhat.com/errata/RHSA-2020:5500
https://access.redhat.com/errata/RHSA-2020:5503
https://access.redhat.com/errata/RHSA-2020:5506
https://access.redhat.com/errata/RHSA-2020:5526
https://access.redhat.com/errata/RHSA-2020:5527
https://access.redhat.com/errata/RHSA-2020:5528
https://access.redhat.com/errata/RHSA-2020:5529
https://access.redhat.com/errata/RHSA-2020:5533
https://access.redhat.com/errata/RHSA-2020:5554
https://access.redhat.com/errata/RHSA-2020:5561
https://access.redhat.com/errata/RHSA-2020:5562
https://access.redhat.com/errata/RHSA-2020:5563
https://access.redhat.com/errata/RHSA-2020:5564
https://access.redhat.com/errata/RHSA-2020:5565
https://access.redhat.com/errata/RHSA-2020:5566
https://access.redhat.com/errata/RHSA-2020:5567
https://access.redhat.com/errata/RHSA-2020:5568
https://access.redhat.com/errata/RHSA-2020:5581
https://access.redhat.com/errata/RHSA-2020:5583
https://access.redhat.com/errata/RHSA-2020:5585
https://access.redhat.com/errata/RHSA-2020:5586
https://access.redhat.com/errata/RHSA-2020:5588

https://access.redhat.com/errata/RHSA-2020:5599
https://access.redhat.com/errata/RHSA-2020:5605
https://access.redhat.com/errata/RHSA-2020:5606
https://access.redhat.com/errata/RHSA-2020:5607
https://access.redhat.com/errata/RHSA-2020:5608
https://access.redhat.com/errata/RHSA-2020:5609
https://access.redhat.com/errata/RHSA-2020:5611
https://access.redhat.com/errata/RHSA-2020:5619
https://access.redhat.com/errata/RHSA-2020:5620
https://access.redhat.com/errata/RHSA-2020:5623
https://access.redhat.com/errata/RHSA-2020:5625

12. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.348004

13. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20203760-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203761-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203762-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203763-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203764-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203765-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203766-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203781-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203790-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203798-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203799-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203824-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203825-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203830-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203841-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203842-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203843-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203844-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203845-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203863-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203864-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203865-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203866-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203867-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014562-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014563-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014564-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014570-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014571-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014572-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014573-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014578-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014579-1/

14. Trend Micro Interscan Web Security Virtual Appliance

https://success.trendmicro.com/solution/000283077

15. Ubuntu

https://ubuntu.com/security/notices/USN-4658-2
https://ubuntu.com/security/notices/USN-4659-2
https://ubuntu.com/security/notices/USN-4660-2
https://ubuntu.com/security/notices/USN-4666-2
https://ubuntu.com/security/notices/USN-4670-1
https://ubuntu.com/security/notices/USN-4671-1
https://ubuntu.com/security/notices/USN-4672-1

16. VMware

https://www.vmware.com/security/advisories/VMSA-2020-0028.html

17. Xen

https://xenbits.xen.org/xsa/advisory-348.html
https://xenbits.xen.org/xsa/advisory-349.html
https://xenbits.xen.org/xsa/advisory-350.html
https://xenbits.xen.org/xsa/advisory-352.html
https://xenbits.xen.org/xsa/advisory-353.html
https://xenbits.xen.org/xsa/advisory-354.html
https://xenbits.xen.org/xsa/advisory-356.html
https://xenbits.xen.org/xsa/advisory-358.html
https://xenbits.xen.org/xsa/advisory-359.html

Sources of product vulnerability information:

Apple
CentOS
Citrix
Debian
F5
Huawei
IBM
Oracle Linux
Red Hat
Slackware
SUSE
SUSE
Trend Micro
Ubuntu
US-CERT
VMware
Xen

Contact:

cert@govcert.gov.hk