GovCERT.HK

Weekly IT Security News Bulletin, 2021-W41

11 October – 17 October 2021

Headlines

NSA warning of heightened wildcard TLS certificate risk

- Researchers warned that using wildcard Transport Layer Security (TLS) certificates to authenticate both HTTP and non-HTTP servers could pose a risk to an application layer protocol content confusion attack dubbed ALPACA. The U.S. National Security Agency (NSA) recently published a guide to help organisations better secure the use of wildcard TLS certificates to verify identities of their servers during handshaking.

- A wildcard certificate is a public key certificate designed to secure all first-level subdomains of a domain name (e.g. *.example.com). The ALPACA attack allows a man-in-the-middle attacker to intercept and manipulate the HTTPS traffic of a web application through non-HTTP services (e.g. FTP, IMAP) which are secured using the same wildcard certificate. A successful attack could lead to information leakage or arbitrary JavaScript code execution in the context of the vulnerable web server.

- To mitigate security risks from the attack, some browser vendors have implemented defenses inside their web browsers, such as blocking more non-HTTP ports and disabling content-sniffing for HTTP requests to non-standard ports.

Advice

- Understand the scope of each wildcard certificate used for websites and web applications.
- Use an application gateway or Web Application Firewall (WAF) in front of servers, including non-HTTP servers.
- Enable Application-Layer Protocol Negotiation (APLN) to allow the server/application to specify permitted protocols where possible.

Sources

- NSA
- Venafi
- BleepingComputer
- ALPACA

Including security in employee offboarding

- Security researchers from ESET published an article to remind organisations about security threats while off-boarding employees. Organisations that have embraced remote or hybrid working environments usually allow employees to access their cloud-based applications, data stores, and other corporate network resources remotely. A remote working environment without proper security measures in place could create conditions for ex-employees to access the organisation's data after the end of employment.

- These insider threats could cause reputational damage to the affected organisations, as well as seriously impacting their financial performance and competitive advantage. To better manage security risks posed by the improper handling of off-boarding employees, establishing a formal written policy and clear procedure could help organisations to clarify the ownership of intellectual property of work data and forbid employees from taking work data when they resign or are terminated.

Advice

- Define a clear termination of employment policy and procedure.
- Revoke departing employee's accesses to all corporate networks, reset their passwords on any shared accounts, and transfer corresponding system ownership.
- Collect all issued devices such as computers, mobile devices, and external storage devices before the employee leaves the organisation.
- Conduct an exit interview to remind all legal obligations and comply with the non-disclosure agreement.

Sources

- WeLiveSecurity

Product Vulnerability Notes & Security Updates

1. Advantech Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-285-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-285-02

2. AMD Products

https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1017

3. Apache Products

https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.72
https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.54
https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.12
https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.0-M6
https://www.openoffice.org/security/cves/CVE-2021-41830.html
https://www.openoffice.org/security/cves/CVE-2021-41831.html
https://www.openoffice.org/security/cves/CVE-2021-41832.html

4. Debian

https://www.debian.org/security/2021/dsa-4982
https://www.debian.org/security/2021/dsa-4983
https://www.debian.org/security/2021/dsa-4984
https://www.debian.org/security/2021/dsa-4985

5. F5 Products

https://support.f5.com/csp/article/K72382141

6. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210922-01-cmd-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-cloudengine-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211008-01-share-en

7. Intel Products

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00544.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00548.html

8. Juniper Products

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11210
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11211
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11212
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11213
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11215
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11216
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11217
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11218
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11219
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11220
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11221
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11222
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11223
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11224
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11225
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11226
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11227
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11228
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11229
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11230
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11231
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11232
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11234
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11235
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11236
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11237
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11238
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11239
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11240
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11241
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11242
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11243
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11244
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11245
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11246
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11247
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11248
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11250
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11251
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11253
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11254
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11255
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11256

9. Mitsubishi Electric MELSEC iQ-R Series

https://us-cert.cisa.gov/ics/advisories/icsa-21-287-03

10. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4KJIY3NX4MIKAMIQIFUSKB4JVJBMJUFI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/7NL4I6R5WB6N3LAJGL2UC3TXXGKBNRLE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/BBFMOSZDI3WFGNU3EM54DUBD3HAM2LEV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FGCILKKE7TLKATFOFTDHZ573UHODPDOM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GDJ2M5H37726GXT3YZBJRSXV3JYGN7CL/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GVBNGQ7UFOBASFEEHWPUJV3UG7BWUIRH/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/H64LCXMISTZ7YB7R4ABO2Y73X23DJFXU/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HHADPIKH543AF7C3D6N7XU3ZL56DUAOW/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HTH54PEZGDIX6ARBBWVMMOYRGAQTP7DV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/INI43FXSUMMTXNS6C5B5BMMQ7XCYCZAV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/MCSKB4ZMNVGFIMLLPPNFDQMFKY7DLL4L/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/MHXVHXC6JGHDS7W6EJQF3JKAPVYH3ES5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/S6VFR2SEGRR5ORYTWSFNBKWUUVDDXFEW/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/TUAORD5DVNESTJH3EH3OO36VCU4DKEPQ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/UVTWOLS4UPD33IXPVQJEU4V4GYL3Z2J7/

11. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-3755.html
https://linux.oracle.com/errata/ELSA-2021-3771.html
https://linux.oracle.com/errata/ELSA-2021-3798.html
https://linux.oracle.com/errata/ELSA-2021-3801.html
https://linux.oracle.com/errata/ELSA-2021-3807.html
https://linux.oracle.com/errata/ELSA-2021-3810.html
https://linux.oracle.com/errata/ELSA-2021-3816.html
https://linux.oracle.com/errata/ELSA-2021-3856.html
https://linux.oracle.com/errata/ELSA-2021-9473.html
https://linux.oracle.com/errata/ELSA-2021-9474.html
https://linux.oracle.com/errata/ELSA-2021-9475.html
https://linux.oracle.com/errata/ELSA-2021-9478.html
https://linux.oracle.com/errata/ELSA-2021-9485.html
https://linux.oracle.com/errata/ELSA-2021-9486.html
https://linux.oracle.com/errata/ELSA-2021-9487.html
https://linux.oracle.com/errata/ELSA-2021-9488.html

12. Red Hat

https://access.redhat.com/errata/RHSA-2021:3754
https://access.redhat.com/errata/RHSA-2021:3755
https://access.redhat.com/errata/RHSA-2021:3756
https://access.redhat.com/errata/RHSA-2021:3757
https://access.redhat.com/errata/RHSA-2021:3766
https://access.redhat.com/errata/RHSA-2021:3768
https://access.redhat.com/errata/RHSA-2021:3769
https://access.redhat.com/errata/RHSA-2021:3770
https://access.redhat.com/errata/RHSA-2021:3771
https://access.redhat.com/errata/RHSA-2021:3791
https://access.redhat.com/errata/RHSA-2021:3798
https://access.redhat.com/errata/RHSA-2021:3801
https://access.redhat.com/errata/RHSA-2021:3802
https://access.redhat.com/errata/RHSA-2021:3810
https://access.redhat.com/errata/RHSA-2021:3811
https://access.redhat.com/errata/RHSA-2021:3812
https://access.redhat.com/errata/RHSA-2021:3814
https://access.redhat.com/errata/RHSA-2021:3816
https://access.redhat.com/errata/RHSA-2021:3818
https://access.redhat.com/errata/RHSA-2021:3819
https://access.redhat.com/errata/RHSA-2021:3836
https://access.redhat.com/errata/RHSA-2021:3837
https://access.redhat.com/errata/RHSA-2021:3851
https://access.redhat.com/errata/RHSA-2021:3856
https://access.redhat.com/errata/RHSA-2021:3871
https://access.redhat.com/errata/RHSA-2021:3872
https://access.redhat.com/errata/RHSA-2021:3873
https://access.redhat.com/errata/RHSA-2021:3874

13. Schneider Electric Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-285-03
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-01

14. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-287-04
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-05
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-06
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-07
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-08
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-09

15. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.483439

16. **SonicWall Products**

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0019

17. **SUSE**

https://www.suse.com/support/update/announcement/2021/suse-su-20213205-2/
https://www.suse.com/support/update/announcement/2021/suse-su-20213323-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213325-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213331-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213332-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213333-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213334-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213335-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213336-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213337-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213338-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213339-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213348-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213350-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213351-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213352-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213353-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213354-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213360-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213361-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213371-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213374-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213385-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213386-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213387-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213388-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213389-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213401-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213415-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213440-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213443-1/

18. **Trend Micro**

https://success.trendmicro.com/solution/000289229
https://success.trendmicro.com/solution/000289230

19. **Ubuntu**

https://ubuntu.com/security/notices/USN-5078-3
https://ubuntu.com/security/notices/USN-5108-1

20. **Uffizio GPS Tracker**

https://us-cert.cisa.gov/ics/advisories/icsa-21-287-02

21. VMware

https://www.vmware.com/security/advisories/VMSA-2021-0021.html
https://www.vmware.com/security/advisories/VMSA-2021-0022.html
https://www.vmware.com/security/advisories/VMSA-2021-0023.html

Sources of product vulnerability information:

AMD
Apache OpenOffice
Apache Tomcat
Debian
F5 Products
Huawei
Intel
Juniper
openSUSE
Oracle Linux
Red Hat
Slackware
SonicWall
SUSE
Trend Micro
Ubuntu
US-CERT
VMware

Contact:

cert@govcert.gov.hk