GovCERT.HK

Weekly IT Security News Bulletin, 2021-W03

18 January – 24 January 2021

Headlines

Hacking e-readers through multiple vulnerabilities

- A security researcher discovered a way to remotely compromise Amazon Kindle, a popular e-reader, by exploiting three different vulnerabilities in the device through a chained attack.

- Kindle has a feature called "Send to Kindle" which allows users to share e-books to their devices as email attachments to specific kindle email addresses from predefined approved emails. Without proper authentication on email senders, a hacker can send malicious e-book to victim's Kindle. When the victim opens the e-book and click on the links in it, a malicious JPEG image file will be opened, causing buffer overflow when the image is parsed. The hacker can then execute arbitrary code and escalate privileges and run code as root on the device.

- By executing malicious code on the device, the hacker may steal the device credentials and use victims' credit card for purchases on Kindle store and get financial gains by selling the e-books.

- Upon receiving the report from the researcher, Amazon has released an update to fix the vulnerabilities.

Advice

- Do not open ebook from any unknown source.
- Apply security patch on your device in a timely manner.
- Email service providers should verify email senders through proper email authentication mechanisms like SPF and DKIM.

Sources

- Security Blog
- Security Affairs

DDoS attacks through RDP services

- The Microsoft Remote Desktop Protocol (RDP) services are widely used in various organisations to support remote work amid the epidemic. However, a security vendor is warning that RDP can be exploited by malicious actors to perform large scale distributed denial-of-service (DDoS) attacks.

- To launch a DDoS attack, an attacker sends amplification traffic with UDP packets originated from port 3389 to target an IP address and UDP port of the attacker's choice. By abusing the RDP services, an attacker can achieve a huge amplification ratio of 85.9:1 through UDP-based amplification attacks. The security vendor identified that about 33,000 RDP servers could potentially be exploited for DDoS attacks. A rising trend of RDP DDoS attack has been observed and it is now being employed in DDoS-for-hire services, making it more accessible to malicious actors.

Advice

- Only allow RDP services to be accessed via VPN to avoid being abused.
- Stop using UDP port 3389 for RDP services as an interim measure.
- Set up policy and controls on network traffic and restrict the traffic to and from the Internet.

Sources

- Netscout
- Threatpost

Product Vulnerability Notes & Security Updates

1. CentOS

https://lists.centos.org/pipermail/centos-announce/2021-January/048243.html

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-5PAZ3hRV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr-mem-leak-dos-MTWGHKk3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-sc-Jd42D4Tq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-sqi-h5fDvZWp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssmor-MDCWkT2x
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-api-path-TpTApx2p
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-authbypass-OHBPbxu
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-cert-check-BdZZV9T3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-info-disc-QCSJB6YG
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-sql-inj-OAQOObP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-ssrf-F2vX6q5p
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-xss-vulns-GuUJ39gh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-cmdinj-erumsWh9
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-csrf-dC83cMcV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-6qjA3hVh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnacid-OfeeRjcn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnsmasq-dns-2021-c5mrdf3q
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-RHp44vAC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esc-dos-4Gw6D527
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-trav-inj-dM687ZD6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-2-UPO232DG
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vinfdis-MC8L58dj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umb-dos-dgKzDEBP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-pathtrav-Z5mCVsjf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-sqlinjm-xV8dsjq5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-cql-inject-72EhnUc

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-xss-RuB5WGqL

3. **Debian**

https://www.debian.org/security/2021/dsa-4830
https://www.debian.org/security/2021/dsa-4831
https://www.debian.org/security/2021/dsa-4832
https://www.debian.org/security/2021/dsa-4833

4. **Delta Electronics Products**

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-02

5. **Dnsmasq by Simon Kelley**

https://us-cert.cisa.gov/ics/advisories/icsa-21-019-01

6. **F5 F5OS**

https://support.f5.com/csp/article/K28563873

7. **Gentoo Linux**

https://security.gentoo.org/glsa/202101-11

8. **Google Chrome**

https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html

9. **Honeywell OPC UA Tunneller**

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-03

10. **Huawei Products**

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-01-http-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-02-privilege-en

11. **Microsoft Edge (Chromium-based)**

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-21-2021

12. **Mitsubishi Electric MELFA**

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-04

13. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-0094.html
https://linux.oracle.com/errata/ELSA-2021-0095.html
https://linux.oracle.com/errata/ELSA-2021-0150.html
https://linux.oracle.com/errata/ELSA-2021-0153.html
https://linux.oracle.com/errata/ELSA-2021-0162.html

14. Red Hat

https://access.redhat.com/errata/RHSA-2021:0034
https://access.redhat.com/errata/RHSA-2021:0037
https://access.redhat.com/errata/RHSA-2021:0038
https://access.redhat.com/errata/RHSA-2021:0039
https://access.redhat.com/errata/RHSA-2021:0079
https://access.redhat.com/errata/RHSA-2021:0150
https://access.redhat.com/errata/RHSA-2021:0151
https://access.redhat.com/errata/RHSA-2021:0152
https://access.redhat.com/errata/RHSA-2021:0153
https://access.redhat.com/errata/RHSA-2021:0154
https://access.redhat.com/errata/RHSA-2021:0155
https://access.redhat.com/errata/RHSA-2021:0156
https://access.redhat.com/errata/RHSA-2021:0161
https://access.redhat.com/errata/RHSA-2021:0162
https://access.redhat.com/errata/RHSA-2021:0163
https://access.redhat.com/errata/RHSA-2021:0164
https://access.redhat.com/errata/RHSA-2021:0165
https://access.redhat.com/errata/RHSA-2021:0166
https://access.redhat.com/errata/RHSA-2021:0167
https://access.redhat.com/errata/RHSA-2021:0181
https://access.redhat.com/errata/RHSA-2021:0183
https://access.redhat.com/errata/RHSA-2021:0184
https://access.redhat.com/errata/RHSA-2021:0187
https://access.redhat.com/errata/RHSA-2021:0189
https://access.redhat.com/errata/RHSA-2021:0190

15. Reolink P2P Cameras

https://us-cert.cisa.gov/ics/advisories/icsa-21-019-02

16. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210133-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210139-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210142-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210143-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210153-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210155-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210156-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210158-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210162-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210163-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210166-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20210172-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210175-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210176-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210182-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210183-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210184-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210185-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210186-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114598-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114603-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114604-1/

17. Ubuntu

https://ubuntu.com/security/notices/USN-4689-3
https://ubuntu.com/security/notices/USN-4689-4
https://ubuntu.com/security/notices/USN-4695-1
https://ubuntu.com/security/notices/USN-4696-1
https://ubuntu.com/security/notices/USN-4697-1
https://ubuntu.com/security/notices/USN-4697-2
https://ubuntu.com/security/notices/USN-4698-1
https://ubuntu.com/security/notices/USN-4699-1
https://ubuntu.com/security/notices/USN-4700-1

18. WAGO M&M Software fdtCONTAINER

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05

Sources of product vulnerability information:

CentOS
Cisco
Debian
F5
Gentoo Linux
Google Chrome
Huawei
Microsoft
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk