GovCERT.HK

Weekly IT Security News Bulletin, 2022-W30 (*25 July – 31 July*)

Headlines

Be aware of malicious Internet Information Services (IIS) extensions

- According to a recent report, attackers are increasingly leveraging Internet Information Services (IIS) extensions to maintain persistence on compromised servers. Malicious IIS extensions are less frequently encountered in attacks against servers, with attackers often only using web shells as the first stage payload. This leads to a relatively lower detection rate for malicious IIS extensions compared to web shells.

- Typically, attackers first exploit a critical vulnerability in the hosted application for initial access before dropping a web shell as the first stage payload. To provide covert and persistent access to the server, the attackers then install malicious IIS extensions. Attackers can also install customized IIS modules according to their objectives.

- These malicious IIS extensions are hard to detect since they often reside in the same directories as legitimate modules used by target applications and follow the identical code structure as other IIS extensions.

Advice

- Ensure systems and software are up to date to prevent exploitation of known vulnerabilities.
- Monitor Windows events or network logs for abnormal or suspicious activities.
- Regular inspect IIS configuration and the list of installed modules of hosted application for suspicious additions.

Sources

- Microsoft
- BleepingComputer

Attackers pivot around Microsoft's announcements to block macros by default

- Security researchers observed that threat actors were changing their malware distribution tactics in response to the announcements by Microsoft in blocking Excel 4.0 (XL4) and Visual Basic for Applications (VBA) macros by default for Office applications.

- With Microsoft beginning to block VBA macros based on a Mark of the Web (MOTW) attribute that shows whether a file comes from the Internet, threat actors were trying to bypass such detection via container files such as ISO and IMG files. By repackaging the Office documents with malicious macros into container files, the system will not identify the document as coming from the web so that threat actors can bypass the macro-blocking feature.

- After Microsoft rolled out the macro-blocking, the number of campaigns leveraging container file formats had surged by nearly 175% and the use of macros in campaigns was decreased by 66% between October 2021 and June 2022.

Advice

- Stay vigilant against unsolicited emails and avoid opening any suspicious or unexpected attachments.
- Use robust endpoint security solutions and scan emails and web content for malicious payloads.
- Be aware of the latest trends and imminent threats of malware variants and adopt security measures to mitigate the risks.

Sources

- Proofpoint
- BleepingComputer

Product Vulnerability Notes & Security Updates

1. **Atlassian**

   https://confluence.atlassian.com/doc/confluence-security-advisory-2022-07-20-1142446709.html

2. **Citrix**

   https://support.citrix.com/article/CTX457836

3. **Debian**

   https://www.debian.org/security/2022/dsa-5186
   https://www.debian.org/security/2022/dsa-5187
   https://www.debian.org/security/2022/dsa-5188
   https://www.debian.org/security/2022/dsa-5189
   https://www.debian.org/security/2022/dsa-5190
   https://www.debian.org/security/2022/dsa-5191
   https://www.debian.org/security/2022/dsa-5192
   https://www.debian.org/security/2022/dsa-5193

4. **F5 Products**

   https://support.f5.com/csp/article/K08152433

5. **Honeywell Products**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-207-02
   https://us-cert.cisa.gov/ics/advisories/icsa-22-207-03

6. **Inductive Automation Ignition**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-207-01

7. **McAfee**

   https://kcm.trellix.com/corporate/index?page=content&id=SB10368
   https://kcm.trellix.com/corporate/index?page=content&id=SB10381
   https://kcm.trellix.com/corporate/index?page=content&id=SB10384
   https://kcm.trellix.com/corporate/index?page=content&id=SB10385

8. **MOXA NPort 5110**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-207-04

9. **openSUSE**

   https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3WZIAKQR5DLQIK63UIUTGPPJ3RM36QHK/
   https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4YEBNCIRQOKETS4R7J5GXRP3TKF2YKFJ/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5X3TQUI5WB3K2BL4Z62ZLZ4Q6ZSIWBC4/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/365XX4K3GWL5IQIIBELCA2CL5KWYJZP7/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/CVD6H5GQOS7AWFJTZ5J55YHOLW4IKGMD/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FRJULJZCSX3FXZZPMZVSL6JYC7UN7YXL/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/H72NRWXOTSJIR4DONVTBYZNQDXZNPXJE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HCR7HUTOWF4KGW66ZVKP6ZLD226PQDDK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LPLR6XKHSXBARGUVHBD2LN3EVYWUJGXH/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/M2J5I4SMKZ66BAR36QD4HWFIOUHNJQEY/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/M7MWG7KVN226XKCGY5HO5W2SNOHSAO4T/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/MUBDJCH5DQPJ7XOEJZUNCPQIWVNBR4ND/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/NKMODULLLGNO53TFOVPVI4VQJE36HLFN/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/NUEMLY7SQDK6SNHOUBMMAUR4U7BC75YW/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/PBSNI6MLTLRF2V2WOHBE2MAHYOMEZU4F/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/PDFZMZPVURR62SMJ3JMOD6NHRBNQHQCR/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/PTD5PFC7675RYBLUMZNIRNJABGNM6SQM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/QEML6RS6UMHDYGJ355BS2ARODQ4OYLRW/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SZO4VKCA4Q5REXHW7HRN3BGFWGLMGTGM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/VTITXJMVTZHOHZFSBGI6AMANQWHYZYE6/

10. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-5696.html
https://linux.oracle.com/errata/ELSA-2022-5698.html
https://linux.oracle.com/errata/ELSA-2022-5717.html
https://linux.oracle.com/errata/ELSA-2022-5726.html

11. Red Hat

https://access.redhat.com/errata/RHSA-2022:5664
https://access.redhat.com/errata/RHSA-2022:5678
https://access.redhat.com/errata/RHSA-2022:5681
https://access.redhat.com/errata/RHSA-2022:5683
https://access.redhat.com/errata/RHSA-2022:5684
https://access.redhat.com/errata/RHSA-2022:5685
https://access.redhat.com/errata/RHSA-2022:5687

https://access.redhat.com/errata/RHSA-2022:5695
https://access.redhat.com/errata/RHSA-2022:5696
https://access.redhat.com/errata/RHSA-2022:5697
https://access.redhat.com/errata/RHSA-2022:5698
https://access.redhat.com/errata/RHSA-2022:5699
https://access.redhat.com/errata/RHSA-2022:5700
https://access.redhat.com/errata/RHSA-2022:5701
https://access.redhat.com/errata/RHSA-2022:5702
https://access.redhat.com/errata/RHSA-2022:5703
https://access.redhat.com/errata/RHSA-2022:5704
https://access.redhat.com/errata/RHSA-2022:5709
https://access.redhat.com/errata/RHSA-2022:5716
https://access.redhat.com/errata/RHSA-2022:5717
https://access.redhat.com/errata/RHSA-2022:5718
https://access.redhat.com/errata/RHSA-2022:5719
https://access.redhat.com/errata/RHSA-2022:5720
https://access.redhat.com/errata/RHSA-2022:5726
https://access.redhat.com/errata/RHSA-2022:5736
https://access.redhat.com/errata/RHSA-2022:5738
https://access.redhat.com/errata/RHSA-2022:5753
https://access.redhat.com/errata/RHSA-2022:5755
https://access.redhat.com/errata/RHSA-2022:5756
https://access.redhat.com/errata/RHSA-2022:5757
https://access.redhat.com/errata/RHSA-2022:5758
https://access.redhat.com/errata/RHSA-2022:5759

12. Rockwell Products

https://us-cert.cisa.gov/ics/advisories/icsa-22-209-01

13. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.352676
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.366703
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.418175

14. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20222522-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222523-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222524-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222525-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222526-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222527-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222529-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222530-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222531-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222532-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222533-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222535-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20222536-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222537-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222539-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222540-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222543-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222546-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222547-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222549-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222550-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222551-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222552-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222553-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222557-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222560-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222561-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222562-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222565-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222566-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222567-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222568-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222569-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222574-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222575-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222577-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222578-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222580-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222581-1/

15. Trend Micro

https://success.trendmicro.com/solution/000291267

16. Ubuntu

https://ubuntu.com/security/notices/USN-5530-1
https://ubuntu.com/security/notices/USN-5531-1
https://ubuntu.com/security/notices/USN-5532-1
https://ubuntu.com/security/notices/USN-5533-1
https://ubuntu.com/security/notices/USN-5534-1
https://ubuntu.com/security/notices/USN-5535-1
https://ubuntu.com/security/notices/USN-5536-1
https://ubuntu.com/security/notices/USN-5537-1
https://ubuntu.com/security/notices/USN-5537-2
https://ubuntu.com/security/notices/USN-5538-1
https://ubuntu.com/security/notices/USN-5539-1
https://ubuntu.com/security/notices/USN-5540-1
https://ubuntu.com/security/notices/USN-5541-1

17. Xen

https://xenbits.xen.org/xsa/advisory-408.html

Sources of product vulnerability information:

- Citrix
- Debian
- F5 Products
- McAfee
- openSUSE
- Oracle Linux
- Red Hat
- Slackware
- SUSE
- Trend Micro
- Ubuntu
- US-CERT
- Xen

Contact:

cert@govcert.gov.hk

Release Date:

1 August 2022