ACTIVITY ALERT

Joint Activity Alert

AA20-133A NUMBER

May 12, 2020 DATE

Top 10 Routinely Exploited Vulnerabilities

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

This alert provides details on vulnerabilities routinely exploited by foreign cyber actors—primarily Common Vulnerabilities and Exposures (CVEs)[1]—to help organizations reduce the risk of these foreign threats.

Foreign cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations. Exploitation of these vulnerabilities often requires fewer resources as compared with zero-day exploits for which no patches are available.

The public and private sectors could degrade some foreign cyber threats to U.S. interests through an increased effort to patch their systems and implement programs to keep system patching up to date. A concerted campaign to patch these vulnerabilities would introduce friction into foreign adversaries' operational tradecraft and force them to develop or acquire exploits that are more costly and less widely effective. A concerted patching campaign would also bolster network security by focusing scarce defensive resources on the observed activities of foreign adversaries.

For Malware Initial Finding Reports and Malware Analysis reports associated with the CVEs in this alert, see https://www.us-cert.gov/ncas/alerts/aa20-133a.

[1] https://cve.mitre.org/cve/

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

TECHNICAL DETAILS

Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.

- According to U.S. Government technical analysis, malicious cyber actors most often exploited vulnerabilities in Microsoft's Object Linking and Embedding (OLE) technology. OLE allows documents to contain embedded content from other applications such as spreadsheets. After OLE the second-most-reported vulnerable technology was a widespread Web framework known as Apache Struts.
- Of the top 10, the three vulnerabilities used most frequently across state-sponsored cyber actors from China, Iran, North Korea, and Russia are CVE-2017-11882, CVE-2017-0199, and CVE-2012-0158. All three of these vulnerabilities are related to Microsoft's OLE technology.
- As of December 2019, Chinese state cyber actors were frequently exploiting the same vulnerability—CVE-2012-0158—that the U.S. Government publicly assessed in 2015 was the most used in their cyber operations.[2] This trend suggests that organizations have not yet widely implemented patches for this vulnerability and that Chinese state cyber actors may continue to incorporate dated flaws into their operational tradecraft as long as they remain effective.
- Deploying patches often requires IT security professionals to balance the need to mitigate vulnerabilities with the need for keeping systems running and ensuring installed patches are compatible with other software. This can require a significant investment of effort, particularly when mitigating multiple flaws at the same time.
- A U.S. industry study released in early 2019 similarly discovered that the flaws malicious cyber actors exploited the most consistently were in Microsoft and Adobe Flash products, probably because of the widespread use of these technologies.[3] Four of the industry study's top 10 most exploited flaws also appear on this Alert's list, highlighting how U.S. Government and private-sector data sources may complement each other to enhance security.

Vulnerabilities Exploited in 2020

In addition to the top 10 vulnerabilities from 2016 to 2019 listed above, the U.S. Government has reported that the following vulnerabilities are being routinely exploited by sophisticated foreign cyber actors in 2020:

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
  - An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.
  - An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious

[2] https://www.us-cert.gov/ncas/alerts/TA15-119A

[3] https://www.recordedfuture.com/top-vulnerabilities-2019/

cyber actors are targeting organizations whose hasty deployment of Microsoft O365 may have led to oversights in security configurations and vulnerable to attack.
- Cybersecurity weaknesses—such as poor employee education on social engineering attacks and a lack of system recovery and contingency plans—have continued to make organizations susceptible to ransomware attacks in 2020.

MITIGATIONS

This Alert provides mitigations for each of the top vulnerabilities identified above. In addition to the mitigations listed below, CISA, FBI, and the broader U.S. Government recommend that organizations transition away from any end-of-life software.

Mitigations for the Top 10 Most Exploited Vulnerabilities 2016–2019

Note: The lists of associated malware corresponding to each CVE below is not meant to be exhaustive but instead is intended to identify a malware family commonly associated with exploiting the CVE.

CVE-2017-11882

- Vulnerable Products: Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016 Products
- Associated Malware: Loki, FormBook, Pony/FAREIT
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2017-11882

CVE-2017-0199

- Vulnerable Products: Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016, Vista SP2, Server 2008 SP2, Windows 7 SP1, Windows 8.1
- Associated Malware: FINSPY, LATENTBOT, Dridex
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2017-0199

CVE-2017-5638

- Vulnerable Products: Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1
- Associated Malware: JexBoss
- Mitigation: Upgrade to Struts 2.3.32 or Struts 2.5.10.1
- More Detail:
  - https://www.us-cert.gov/ncas/analysis-reports/AR18-312A
  - https://nvd.nist.gov/vuln/detail/CVE-2017-5638

CVE-2012-0158

- Vulnerable Products: Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0
- Associated Malware: Dridex
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail:
  - https://www.us-cert.gov/ncas/alerts/aa19-339a
  - https://nvd.nist.gov/vuln/detail/CVE-2012-0158

CVE-2019-0604

- Vulnerable Products: Microsoft SharePoint
- Associated Malware: China Chopper
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2019-0604

CVE-2017-0143

- Vulnerable Products: Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016
- Associated Malware: Multiple using the EternalSynergy and EternalBlue Exploit Kit
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2017-0143

CVE-2018-4878

- Vulnerable Products: Adobe Flash Player before 28.0.0.161
- Associated Malware: DOGCALL
- Mitigation: Update Adobe Flash Player installation to the latest version
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2018-4878

CVE-2017-8759

- Vulnerable Products: Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7
- Associated Malware: FINSPY, FinFisher, WingBird
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2017-8759

CVE-2015-1641

- Vulnerable Products: Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1
- Associated Malware: Toshliph, UWarrior
- Mitigation: Update affected Microsoft products with the latest security patches
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2015-1641

CVE-2018-7600

- Vulnerable Products: Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1
- Associated Malware: Kitty
- Mitigation: Upgrade to the most recent version of Drupal 7 or 8 core.
- More Detail: https://nvd.nist.gov/vuln/detail/CVE-2018-7600

Mitigations for Vulnerabilities Exploited in 2020

CVE-2019-11510

- Vulnerable Products: Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 and Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15
- Mitigation: Update affected Pulse Secure devices with the latest security patches.
- More Detail:
  - https://www.us-cert.gov/ncas/alerts/aa20-107a
  - https://nvd.nist.gov/vuln/detail/CVE-2019-11510
  - https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

CVE-2019-19781

- Vulnerable Products: Citrix Application Delivery Controller, Citrix Gateway, and Citrix SDWAN WANOP
- Mitigation: Update affected Citrix devices with the latest security patches
- More Detail:
  - https://www.us-cert.gov/ncas/alerts/aa20-020a
  - https://www.us-cert.gov/ncas/alerts/aa20-031a
  - https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability.html
  - https://nvd.nist.gov/vuln/detail/CVE-2019-19781
  - https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

Oversights in Microsoft O365 Security Configurations

- Vulnerable Products: Microsoft O365
- Mitigation: Follow Microsoft O365 security recommendations
- More Detail: https://www.us-cert.gov/ncas/alerts/aa20-120a

Organizational Cybersecurity Weaknesses

- Vulnerable Products: Systems, networks, and data
- Mitigation: Follow cybersecurity best practices
- More Detail: https://www.cisa.gov/cyber-essentials

CISA's Free Cybersecurity Services

Adversaries use known vulnerabilities and phishing attacks to compromise the security of organizations. CISA offers several free scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

Cyber Hygiene: Vulnerability Scanning helps secure your internet-facing systems from weak configuration and known vulnerabilities. It also encourages organizations to adopt modern security best practices. CISA performs regular network and vulnerability scans and delivers a weekly report for your action. Once initiated, this service is mostly automated and requires little direct interaction. After CISA

receives the required paperwork for Cyber Hygiene, our scans will start within 72 hours and you'll begin receiving reports within two weeks.

Web Application Service checks your publicly accessible web sites for potential bugs and weak configurations. It provides a "snapshot" of your publicly accessible web applications and also checks functionality and performance in your application.

If your organization would like these services or want more information about other useful services, please email vulnerability_info@cisa.dhs.gov.

CISA Online Resources

The Patch Factory: CISA infographic depicting the global infrastructure for managing vulnerabilities.

CISA Alert: (AA20-120A) Microsoft Office 365 Security Recommendations: recommendations for organizations to review and ensure their O365 environment is configured to protect, detect, and respond against would-be attackers.

CISA's Cyber Essentials: a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

CONTACT INFORMATION

If you have any further questions related to this Joint Alert, please contact the FBI at either your local Cyber Task Force or FBI CyWatch.

- You can find your local field offices at https://www.fbi.gov/contact-us/field
- CyWatch can be contacted through e-mail at cywatch@fbi.gov or by phone at 1-855-292-3937

To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

REFERENCES

[1] MITRE CVE webpage

[2] CISA Alert: (TA15-119A) Top 30 Targeted High Risk Vulnerabilities

[3] Recorded Futures blog, 2019 Vulnerability Report: Cybercriminals Continue to Target Microsoft Products