SERIANU

Serianu Cyber Security Advisory

Top 10 Routinely Exploited Vulnerabilities

Serianu SOC Advisory Number:

TA – 2020/003

Date Issued:

3rd August, 2020

OVERVIEW:

The Serianu research team is sharing this technical guidance to advice IT professionals in organizations, both private and public, to increase priority on patching common vulnerabilities that are increasing being exploited by sophisticated malicious actors. This alert contains Common Vulnerabilities and Exposures (CVEs) routinely exploited by these malicious actors who continue to use these publicly known vulnerabilities to breach both public and private sector organizations.

It is important to note that most malicious actors use publicly known vulnerabilities, rather than zero-day exploits which are costly to research on, and require resources that are not available to many malicious actors. Hence, an increased effort in patching systems and implementing programs to keep system patching up to date will reduce the threat surface in both public and private sectors organizations. An increased focus on patching will also allow organizations to focus on available cyber security resources observing any observed actions from adversaries.

This advisory covers the top exploited vulnerabilities by malicious actors for the period 2016-2020 and suggest mitigations.

Vulnerabilities Exploited in 2020

The shift to work-from-home setups necessitated by the current pandemic has made many organizations to rapidly deploy tools such as cloud collaboration tools such as Office365, VPN appliances etc. This has led to attackers targeting organizations whose hasty deployment of these tools may have led to oversights in security configurations. In addition, with employees working remotely, poor employee sensitization on social engineering attacks continue to leave organizations susceptible to ransomware attacks.

Vulnerabilities and Suggested Mitigations:

1. **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.
2. **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

Oversights in Microsoft Office365 Security Configurations

- Vulnerable Products: Microsoft Office365
- Mitigation: Follow Microsoft Office365 security recommendations

Organizational Cybersecurity Weaknesses

- Vulnerable Products: Systems, networks, and data
- Mitigation: Follow cybersecurity best practices

Vulnerabilities Exploited 2016 - 2019

Most vulnerabilities exploited during this period target widely used technologies such as Microsoft and Adobe products. It was noted that malicious actors are routinely exploiting vulnerabilities published as far back as 2012, showing that some organizations haven't implemented patches for a long time.

Serianu research team advices that as IT security professionals try to balance the need to mitigate vulnerabilities and the need to keep systems running and ensuring patches are compatible with other components, it is important to place additional importance on mitigating vulnerabilities, as some vulnerabilities when exploited have the ability to severely cripple business operations

Vulnerabilities and Suggested Mitigations

1. **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
2. **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
3. **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
4. **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

5. **CVE-2019-0604**
    - Vulnerable Products: Microsoft SharePoint
    - Associated Malware: China Chopper
    - Mitigation: Update affected Microsoft products with the latest security patches
6. **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
7. **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

8. **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
9. **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
10. **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.
    - Mitigation: Follow cybersecurity best practices

Conclusion

Malicious attackers constantly use known vulnerabilities and phishing attacks to compromise the security of organizations. Serianu research team highly recommends that organizations follow cybersecurity best practices and transition from any end-of-life software and hardware. Organizations should also take a proactive approach to mitigating attack vectors by regularly scanning and testing their assets for exposure to threats.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to the top 10 routinely exploited vulnerabilities to share it with us through our email: info@serianu.com.