The Top 11
Routinely Exploited Vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) recently published the list of the Top 10 Routinely Exploited Vulnerabilities from 2016-2019.

The list highlights the vulnerabilities leveraged by foreign cyber actors when targeting both public and private sector organizations. CISA and the FBI have also highlighted several new key trends in adversarial activity in 2020, much of which is driven by new work from home trends.

Since it represents the most common exploits, rather than just high severity vulnerabilities according to CVSS score, you should review this list for your own organization's exposure when trying to assess your organization's breach risk and, ultimately, improve overall security posture.

Here is the full list of the top 11 most exploited vulnerabilities:

1. **CVE-2019-19781**
   Citrix Application Delivery Controller vulnerability
2. **CVE-2018-7600**
   Drupal remote code execution vulnerability.
3. **CVE-2015-1641**
   Microsoft Office memory corruption vulnerability.
4. **CVE-2017-8759**
   Microsoft.NET Framework Remote Code Execution Vulnerability.
5. **CVE-2018-4878**
   Adobe Flash Player vulnerability.
6. **CVE-2017-0143**
   SMB server vulnerability in older versions of Windows and Windows Server.
7. **CVE-2018-7600**
   Remote code execution vulnerability in all modern versions of Sharepoint.
8. **CVE-2012-0158**
   Microsoft Office vulnerability.
9. **CVE-2017-5638**
   Apache Struts vulnerability.
10. **CVE-2017-0199**
    Microsoft Office remote code execution.
11. **CVE-2017-11882**
    Microsoft Office memory corruption vulnerability.

Here are the 6 best ways to protect against the most exploited vulnerabilities:

1 Update old software versions.

5 of the top 10 exploited vulnerabilities impact only old versions of Microsoft software, primarily Microsoft Office OLE components. Another one targets Adobe Flash Player, another end-of-life software package. According to CISA, *"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."*

2 Patch known high and critical CVEs.

Adversaries continue to exploit publicly known CVEs, many of which are quite dated. Two of the top 10 vulnerabilities are more than 5 years old, and another 5 of them are from 2017!

3 Use a risk-based approach to vulnerability management.

There are thousands of reported *"High" and "Critical"* CVEs reported each year, the vast majority of which will never be publicly exploited. Of the top 10 list, only 3 have a CVSS qualitative rating of *"Critical."* Organizations prioritizing vulnerability remediation based on CVSS base score rather than on risk will spend far too many resources on vulnerabilities that will never be exploited, at the expense of vulnerabilities like the ones in this list.

4 Be mindful of security configurations for public cloud applications.

The rapid shift to remote work has resulted in a much broader enterprise attack surface, including an accelerated adoption of cloud applications. According to CISA, *"Malicious cyber actors are targeting organizations whose hasty deployment of Microsoft O365 may have led to oversights in security configurations and vulnerable to attack."* These oversights are not due to the cloud be insecure, but due to the cloud being used insecurely.

5 Ensure that remote access infrastructure is patched.

Two of the most common vulnerabilities being exploited in 2020 target remote access VPN infrastructure—one impacting Pulse Secure products, and the other impacting Citrix remote access products. Both vulnerabilities have been widely reported and there are patches available for impacted products.

6 Continue to assess and improve your overall cybersecurity posture.

CISA highlights that basic cyber hygiene best practices can thwart many attacks, including many state sponsored attacks. *"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."*

A risk-based approach to vulnerability management will ensure that your organization is protected against not only the most common, but the vast majority of attack methods that are in use by both state-sponsored and private adversaries.

READ MORE

Balbix®