TOP CVE'S EXPLOITED IN THE WILD

December 27, 2019

SonicWALL Capture Labs Threat Research team observed the below vulnerabilities most exploited by hackers in the year 2019.

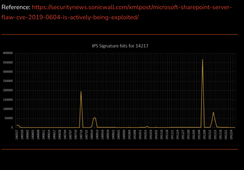
- **BlueKeep (CVE-2019-0708)**
- **SharePoint Server (CVE-2019-0604)**
- **Win32k (CVE-2019-0859)**
- **ThinkPhp (CVE not assigned)**
- **Atlassian Confluence (CVE-2019-3396)**
- **Drupal (CVE-2019-6340)**
- **Oracle WebLogic (CVE-2019-2725)**
- **Exim Server (CVE-2019-10149)**
- **Microsoft GDI (CVE-2019-0903)**
- **Webmin Server (CVE-2019-15107)**

BlueKeep (CVE-2019-0708)

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, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Affected Products: Windows 7, Windows XP, Windows Server 2008 and Windows Server 2003.

Reference: https://securitynews.sonicwall.com/xmlpost/rdp-vulnerability-cve-2019-0708/

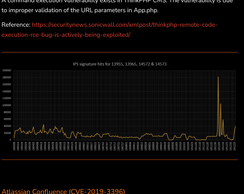


SharePoint Server (CVE-2019-0604)

An insecure deserialization vulnerability has been reported in Microsoft SharePoint Server. This vulnerability is due to insufficient validation user-supplied data to EntityInstanceIdEncoder.

Affected Products:
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2010 & 2013
Microsoft SharePoint Server 2010, 2013 & 2019

Reference: https://securitynews.sonicwall.com/xmlpost/microsoft-sharepoint-server-flaw-cve-2019-0604-is-actively-being-exploited/



Win32k (CVE-2019-0859)

An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.

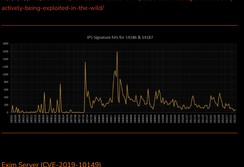
Affected Products:
Microsoft Windows 7, 8.1, 10 & Rt 8.1
Microsoft Windows Server 2008, 2012, 2016 & 2019

Reference: https://securitynews.sonicwall.com/xmlpost/cve-2019-0859-exploits-active-in-the-wild/

ThinkPhp (CVE not assigned)

A command execution vulnerability exists in ThinkPHP CMS. The vulnerability is due to improper validation of the URL parameters in App.php.

Reference: https://securitynews.sonicwall.com/xmlpost/thinkphp-remote-code-execution-rce-bug-is-actively-being-exploited/



Atlassian Confluence (CVE-2019-3396)

A server side template injection vulnerability has been reported in Atlassian Confluence Server. This vulnerability is due to improper validation of the _template JSON parameter.

Affected Products:

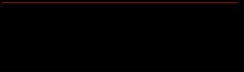
Atlassian Confluence Server 6.14.x prior to 6.14.2
Atlassian Confluence Server 6.13.x prior to 6.13.3
Atlassian Confluence Server 6.12.x prior to 6.12.3
Atlassian Confluence Server 6.6.x prior to 6.6.12

Drupal (CVE-2019-6340)

A remote code execution vulnerability has been reported in the web services components of Drupal Core. The vulnerability is due to improper sanitization of data for certain Field Types from non-form sources prior to deserialization.

Affected Products:

Drupal Drupal 8.5.x prior to 8.5.11
Drupal Drupal 8.6.x prior to 8.6.10
Drupal Drupal 7.x



Oracle WebLogic (CVE-2019-2725)

An insecure deserialization vulnerability has been reported in Oracle Weblogic. This vulnerability is due to insufficient validation of XML data within the body of HTTP POST requests.

Affected Products:

Oracle WebLogic Server 12.1.3.0.0
Oracle WebLogic Server 10.3.6.0.0

Reference: https://securitynews.sonicwall.com/xmlpost/oracle-weblogic-vulnerability-actively-being-exploited-in-the-wild/

Exim Server (CVE-2019-10149)

A remote command execution injection vulnerability has been reported in Exim server. This vulnerability is due to insufficient handling of recipient address in the deliver_message() function.

Affected Products: Exim versions 4.87 to 4.91

Reference: https://securitynews.sonicwall.com/xmlpost/exim-email-servers-are-still-under-attack/

Microsoft GDI (CVE-2019-0903)

A remote code execution vulnerability has been reported in the GDI component of Microsoft Windows. The vulnerability is due to the way that GDI handles objects in memory.

Affected Products:

Microsoft Windows 7, 8.1, 10
Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019

Webmin Server (CVE-2019-15107)

A command injection vulnerability has been reported in Webmin. The vulnerability is due to improper validation of user supplied input within password_change.cgi.

Affected Products: Webmin prior to 1.930

Reference: https://securitynews.sonicwall.com/xmlpost/hackers-continue-to-mount-attacks-on-webmin-servers/