Privasec | RED
RED TEAMING & ADVANCED ETHICAL HACKING

CRITICAL - vBulletin version 5 - Unauthenticated Remote Code Execution (RCE) (CVE-2019-16759) – PATCH IMMEDIATELY

Fact Sheet v1.0 – 27th September 2019

What is vBulletin?

vBulletin is one of the primarily used forum-based software packages on the Internet.

Summary

Recently, an anonymous researcher publicly disclosed exploit code that allows the execution of arbitrary code on vulnerable instances of vBulletin. Most significant is the ability to run this code without providing any form of authentication, meaning this could allow random attackers on the Internet to gain unauthorised access to vulnerable systems.

Affected Versions

vBulletin between versions 5.0.0 to 5.5.4.

What are the impacts

Reports suggest this vulnerability is actively being used by attackers and automated malicious bots on the Internet to exploit vulnerable systems.

As a result, if an attacker successfully exploits this vulnerability, this could lead to:

- Significant access to databases, private messages, credentials and other forms of sensitive information;
- Potentially obtain access to internal network resources through compromised perimeter webservers;
- Defacement or Denial of Service (DoS) conditions to these applications; and/or
- Facilitating of attacks against third parties using the infrastructure in which vBulletin is hosted.

Remediation

While this was initially a zero-day vulnerability (meaning there was no official patch from the vendor), a few hours ago an official patch has been released.

Privasec recommends the following immediate actions:

1. Check and assess your infrastructure and asset registers to determine if you are using vBulletin.

2. If you are running any version between 5.0.0 to 5.4.4, immediately invoke your critical patch management process and install the official update as per the vendors instructions below:

    a. https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4422707-vbulletin-security-patch-released-versions-5-5-2-5-5-3-and-5-5-4
    b. The following official documentation can be used as a guide to upgrade vBulletin: https://forum.vbulletin.com/forum/vbulletin-5-connect/vbulletin-5-installations/4391346-quick-overview-upgrading-vbulletin-connect
    c. The patch can be downloaded from the vBulletin Member area here: http://members.vbulletin.com/patches.php

Finally, Privasec recommends reviewing server and applications logs to detect any form of abnormal activity.

DO YOU REQUIRE ADDITIONAL ASSURANCE?

Privasec can provide you with additional assurance and peace of mind.

If you would like us to review your patching practices, perform a Penetration Test to assess potential vectors of attack or review your current network architecture, please contact us for a personalised quote.

References:

- Official vendor announcement:
    - https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4422707-vbulletin-security-patch-released-versions-5-5-2-5-5-3-and-5-5-4
- CVE details
    - https://nvd.nist.gov/vuln/detail/CVE-2019-16759
- Initial public disclosure
    - https://seclists.org/fulldisclosure/2019/Sep/31

Privasec
GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS
RED RED TEAMING & ADVANCED ETHICAL HACKING
DRONE SEC UAS HACKING, HARDENING & DEFENCE

1800 996 001 (AUS)
+65 6631 8375 (SG)
+603 2788 3709 (MY)
+64 9 222 4725 (NZ)

INFO@PRIVASEC.COM
WWW.PRIVASEC.COM

Australia | Level 2, 64 Clarence St, Sydney, NSW 2000
Level 6, 276 Flinders St, Melbourne, VIC 3000
Level 6, 200 Adelaide St, Brisbane, QLD 4000
Singapore | 5 Shenton Way, UIC Building #10-01 Singapore 068808
Malaysia | L9, Unit 3 Wisma UOA II - 6, Changkat Semantan 50490 KL
New Zealand | Level 4, 17 Albert St Auckland 1010