SPAM-Mails vom Freitag, 6. März 2020 - Hintergründe und technische Erklärung hierzu

Beitrag von „coala“ vom 3. Mai 2020 um 10:22

Servus zusammen,

vom beschriebenen Szenario war ja nicht unsere Community betroffen, auch andere Foren hatten unter diesem Bot zu leiden, weshalb zwischenzeitlich vom Anbieter unserer Forensoftware entsprechende Updates veröffentlicht wurden. Einige Maßnahmen (siehe voriger Beitrag) haben wir ja bereits unmittelbar danach als "Erste Hilfe" manuell umgesetzt, zwischenzeitlich allerdings nun auch nach erfolgter Bereitstellung die entsprechenden Updates eingespielt.

Hier zu eurer Info mal die betreffenden Auszüge von WoltLab.

Grüße

Robert

Missbrauch der Konversationen zur Verteilung von Spam-Nachrichten

Wir sind in den vergangenen Tagen auf einen ausgefeilten Bot aufmerksam geworden, der gezielt auf das Konversations-System ausgerichtet ist, um diesen für Spam-Nachrichten zu missbrauchen. Der Bot arbeitet dabei in zwei Phasen um seine Effizienz zu erhöhen, im ersten Schritt wird die Mitgliederliste ausgelesen, um eine vollständige Liste der Benutzernamen zu erhalten. Anschließend werden in der zweiten Phase die zuvor abgegriffenen Benutzernamen verwendet, um jede einzelnen per Konversation mit der Werbebotschaft anzuschreiben. Darüber hinaus wurde der Bot so gestaltet, dass nach dem Versand die Konversation sofort verlassen wird, um das Limit der aktiven Konversationen zu umgehen.

Um unsere Kunden und deren Nutzer zu schützen, haben wir eine neue Maßnahme implementiert, die einen derartigen Missbraucht verhindert und eine wirksame Verteidigung gegen vergleichbare Angriffsszenarien darstellt. Dazu haben wir in das Konversation-System der WoltLab Suite 3.0, 3.1 und 5.2 eine neue Berechtigung eingebaut, die die Anzahl der gestarteten Konversationen innerhalb eines 24-Stunden-Zeitfensters pro Benutzer begrenzt. Standardmäßig können 10 Konversationen gestartet werden, Administratoren werden standardmäßig von dieser Begrenzung befreit.

Seitenbetreiber können die Begrenzung individuell pro Benutzergruppen konfigurieren, einschließlich dem Spezialwert `-1`, der die Beschränkung für die jeweilige Benutzergruppe

vollständig aufhebt. Der Name der neuen Berechtigung lautet `Maximale Anzahl gestarteter Konversation innerhalb von 24 Stunden`.

E-Mail-Versand von Benutzern an andere Benutzer

Im Standardumfang gibt es eine historisch entstandene Funktion, mit der Benutzer (und je nach Konfiguration auch Gäste) andere Benutzer über ein Formular per E-Mail anschreiben können. Diese Funktion hat in der heutigen Zeit keine fundamentale Bedeutung, wird aber bei der Konfiguration, insbesondere bei Migrationen, leicht übersehen. Das Formular basiert auf den Benutzergruppenrechten, die in früheren Versionen die Nutzung standardmäßig erlaubt haben und schlicht nie umkonfiguriert wurden.

Leider mussten wir feststellen, dass diese Funktion inzwischen für den Spam-Versand missbraucht wird und darüber teils enorme E-Mail-Mengen generiert werden. Wir haben uns daher entschlossen, zwei sofortige Maßnahmen einzuleiten, um das Problem zu entschärfen:

1. Die Benutzergruppenrechte für diese Funktion werden einmalig für alle Gruppen entzogen. Administratoren können die Funktion nach eigenen Ermessen anschließend wieder reaktivieren, auch wenn wir vom Einsatz ausdrücklich abraten müssen.
2. Der Captcha-Schutz des Formulars wirkte sich zuvor nur auf Gäste aus, er wird nun ebenfalls für Benutzer angewendet. Dies ist dadurch das erste Formular, dass einen Captcha-Schutz auch für angemeldete Benutzer erfordert.