

Microsoft Security Response Center: Bewertungssystem für Sicherheitsbulletins (Update vom November 2002)

Engl. Originaltitel: [Microsoft Security Response Center Security Bulletin Severity Rating System \(Revised November 2002\)](#)

Vorrangige Aufgabe des Microsoft Security Response Centers (MSRC) ist es, Kunden beim sicheren Betrieb ihrer Systeme und Netzwerke zu unterstützen. In diesem Zusammenhang prüft das MSRC regelmäßig Berichte von Kunden, die auf eventuelle Schwachstellen in Microsoft Produkten hinweisen. Treffen die Berichte zu, sorgt das MSRC für die Erstellung und Verbreitung der entsprechenden Sicherheitsbulletins und Patches, die die Schwachstellen beseitigen. Ein früherer Artikel mit dem Titel [A Tour of the MSRC](#) (englischsprachig) beschreibt, wie diese Aufgabe im täglichen Betrieb erfüllt wird.

Das MSRC veröffentlicht ein Sicherheitsbulletin für jede Schwachstelle, die eine größere Anzahl von Kunden betreffen könnte. Es spielt dabei keine Rolle, wie unwahrscheinlich oder begrenzt die Auswirkungen tatsächlich sind. Dieser Ansatz, auf möglichst viele Schwachstellen zu reagieren, besitzt aber offenbar eine ungewünschte Nebenwirkung. Den Kunden fällt es zusehends schwer, eindeutig festzustellen, welche Schwachstelle tatsächlich ein Sicherheitsrisiko für sie darstellt.

Die Erfahrung zeigt, dass Hacker bei Angriffen in den seltensten Fällen unbekannte Schwachstellen ausnützen. Stattdessen erfolgen Angriffe meist über Sicherheitslücken, die bereits bekannt sind. In der Regel stehen für diese Lücken auch schon Patches zur Verfügung, die dann allerdings nicht installiert wurden.

Es ist bekannt, dass sich Schwachstellen nicht auf alle Benutzer gleich auswirken. In diesem Dokument wird das Bewertungssystem für die Bedeutung von Sicherheitsbulletins vorgestellt. Dieses System, das wir im November 2002 entsprechend dem Feedback unserer Kunden überarbeitet haben, soll Ihnen die Entscheidung über die Installation von Patches erleichtern. Es zeigt Ihnen, welche Patches Sie unter bestimmten Umständen installieren sollten, um Angriffe auf Ihre Umgebung zu verhindern. Zudem gibt es darüber Auskunft, wie zeitkritisch diese Installationen sind. Mit dem Bewertungssystem kommen wir dem Wunsch zahlreicher Kunden nach, die uns um diese Informationen gebeten haben, damit sie die Risiken für ihre Umgebung besser einschätzen können.

Das Bewertungssystem

Das Bewertungssystem umfasst vier unterschiedliche Bewertungen. Jede Schwachstelle wird dabei einer der folgenden Bewertungen zugeordnet:

Bewertung	Beschreibung
Critical	Eine Schwachstelle, die für die Verbreitung eines Internet-Wurms ausgenützt werden kann, ohne dass hierfür spezielle Aktionen des Benutzers erforderlich sind.
Important	Eine Schwachstelle, deren Ausnützung die Vertraulichkeit, Integrität oder Verfügbarkeit von Benutzerdaten oder anderen Ressourcen gefährden kann.
Moderate	Eine Schwachstelle, die sich aufgrund bestimmter Faktoren (z. B. Standardkonfigurationen, Überprüfungen, technische Komplexität) nur deutlich eingeschränkt für Angriffe ausnützen lässt.
Low	Eine Schwachstelle, die sich nur sehr schwer oder mit minimalen Auswirkungen ausnützen lässt.

Wenn von einer Schwachstelle nur in einer bestimmten Systemumgebung oder bei einem spezifischen Einsatz der Software Gefahr ausgeht, wird dies im Sicherheitsbulletin ausdrücklich erwähnt. Dennoch gilt auch in diesem Fall bei der Bewertung der Ansatz, auf möglichst viele entdeckte Sicherheitslücken möglichst umfassend zu reagieren. Deshalb behandeln wir auch diese nur unter bestimmten Bedingungen auftretenden Schwachstellen so, als seien sie allgemein relevant. Wir gehen so vor, als seien die Sicherheitslücken bekannt und als seien der Code oder die Scripts, mit denen sie sich ausnützen lassen, bereits weit verbreitet.

So nutzen Sie das Bewertungssystem

Wir wenden das neue Bewertungssystem ab sofort auf jedes neu veröffentlichte Sicherheitsbulletin an. Bei kumulativen Patches für mehrere Sicherheitslücken nehmen wir die Bewertung entsprechend der gefährlichsten Schwachstelle vor, die durch den Patch behoben wird. Zusätzlich enthalten diese Bulletins aber auch Einzelbewertungen für jede der behandelten Lücken.

Es ist davon auszugehen, dass mit „Critical“ oder „Important“ bewertete Sicherheitslücken die Installation des entsprechenden Patches erforderlich machen. Mit „Critical“ bewertete Patches sollten dabei möglichst zeitnah installiert werden. Kunden, die von einer mit „Moderate“ oder „Low“ bewerteten Sicherheitslücke betroffen sind, sollten in jedem Fall das zugehörige Sicherheitsbulletin lesen. Auf diese Weise können sie feststellen, ob die beschriebene Sicherheitslücke tatsächlich eine Gefahr für ihre spezifische Konfiguration darstellt. Wir nehmen an, dass mit „Low“ bewertete Schwachstellen im Regelfall eher eine kleinere Zahl von Kunden betreffen.

Das Bewertungssystem soll eine weitestgehend objektive Einschätzung jeder veröffentlichten Schwachstelle zur Verfügung stellen. Wir ermuntern die Kunden jedoch dazu, ihre eigenen Umgebungen zu analysieren und auf dieser Grundlage zu entscheiden, welche Patches für den Schutz ihrer Systeme notwendig sind.

Häufig gestellte Fragen zu den Änderungen am Bewertungssystem vom November 2002 finden Sie [hier](#).