LAGE-INFORMATION

Schwachstellenampel

Produktsicherheit auf einen Blick

Schwachstellen oder Sicherheitslücken in Softwareprodukten stellen eine Bedrohung für die Sicherheit von Computersystemen dar. Um ein Eindringen von Schadsoftware in die eigenen Systeme zu verhindern und Angreifern keine Möglichkeit zur Ausnutzung dieser Schwachstellen zu bieten, ist es daher wichtig, stets die aktuellsten Software- oder Sicherheitspatches zu installieren. Falls keine Patches existieren oder aus organisatorischen oder anderen Gründen nicht zeitnah installiert werden können, müssen andere Gegenmaßnahmen ergriffen werden.

Zielsetzung

Im Rahmen der BSI-Veröffentlichungen zur Cyber-Sicherheit bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Schwachstellenampel einen Indikator, der die aktuelle Sicherheitslage in Bezug auf Software-Schwachstellen in ausgewählter, weit verbreiteter Standardsoftware verdeutlicht. Aufgrund des hohen Verbreitungsgrades dieser Produkte kann die Ausnutzung von darin enthaltenen Sicherheitslücken unter Umständen schwerwiegende und flächendeckende IT-Sicherheitsvorfälle nach sich ziehen.

Derartige Sicherheitslücken werden in der Schwachstellenampel statistisch erfasst und aufbereitet. Die BSI-Bewertung für das jeweilige Produkt basiert auf Anzahl und Schweregrad der Schwachstellen. Die drei Ampelfarben spiegeln dabei den aktuellen Schweregrad aller vorhandenen Schwachstellen für das betroffene Produkt wider.

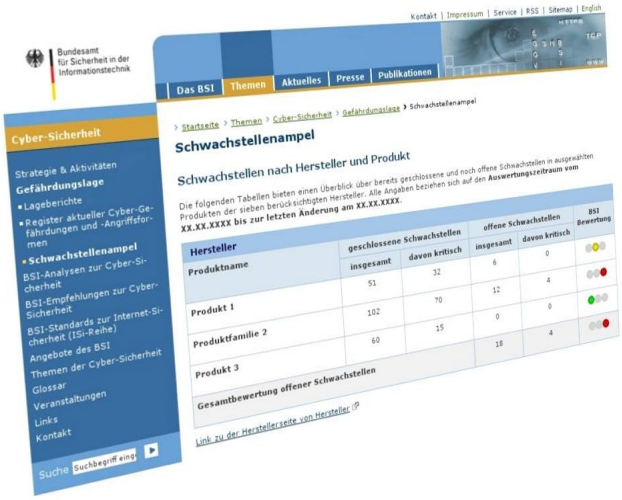

Abbildung 1: Die Schwachstellenampel auf den Internetseiten des BSI

Das vorliegende Dokument aus der Reihe der „BSI-Veröffentlichungen zur Cyber-Sicherheit“ beschreibt ausführlich den Aufbau der Schwachstellenampel sowie deren Funktionsweise und Metriken. Die Schwachstellenampel finden Sie im Internetangebot des BSI unter:
http://www.bsi.bund.de/schwachstellenampel

Aufbau und Funktionsweise der Schwachstellenampel

Auswahl der Softwareprodukte

Die Schwachstellenampel ist ein Indikator, der die aktuelle Sicherheitslage in Bezug auf Sicherheitslücken in gängigen Softwareprodukten verdeutlicht.

Für diese werden derzeit Sicherheitslücken in Produkten der folgenden Hersteller berücksichtigt:

- **Adobe Systems** mit den Produkten Adobe Reader, Adobe Acrobat und Adobe Flash Player
- **Apple Inc.** mit den Produkten Mac OS X, Safari und Quicktime
- **Google Inc.** mit dem Produkt Google Chrome
- der **Linux**-Kernel
- **Microsoft Corporation** mit den Produkten Microsoft Windows, Microsoft Office und Microsoft Internet Explorer
- **Mozilla Foundation** mit den Produkten Mozilla Firefox und Mozilla Thunderbird
- **Oracle Corporation** mit den Produkten Java Development Kit (JDK) und Java Runtime Environment (JRE)

Aufgrund der weiten Verbreitung dieser Produkte in Unternehmen, Behörden und sonstigen Institutionen sowie bei Privatanwendern kann die Ausnutzung von Schwachstellen in diesen Produkten potenziell schwerwiegende und flächendeckende IT-Sicherheitsvorfälle nach sich ziehen. Das BSI behält sich kurzfristige Änderungen der Produktauswahl vor.

Elemente der Schwachstellenampel

Die Schwachstellenampel fasst die Anzahl der Schwachstellen in den berücksichtigten Produkten eines Herstellers jeweils in einer übersichtlichen Tabelle zusammen. In Tabelle 1 wird diese Darstellung am Beispiel eines fiktiven Herstellers „Hersteller“ mit den Produkten 1, 2 und 3 verdeutlicht.

Hersteller					
Produktname	**geschlossene Schwachstellen**		**offene Schwachstellen**		**BSI Bewertung**
	insgesamt	**davon kritisch**	**insgesamt**	**davon kritisch**	
Produkt 1	23	3	1	1	○○●
Produktfamilie 2	17	1	7	0	○●○
Produkt 3	3	0	0	0	●○○
Gesamtbewertung offener Schwachstellen			8	1	○○●

Link zu Sicherheitshinweisen von Hersteller

Tabelle 1: Schwachstellenampel am Beispiel eines fiktiven Herstellers

Der einheitliche Aufbau der Tabellen besteht aus den folgenden Elementen:

Auswertungszeitraum und letzte Änderung

Alle in den Tabellen angegebenen Zahlen beziehen sich ausschließlich auf das oberhalb der ersten Tabelle genannte Datum der letzten Änderung. Der Auswertungszeitraum legt das maximale Alter der für die Statistik zu berücksichtigenden geschlossenen Schwachstellen fest. Schwachstellen, welche vor diesem Zeitpunkt geschlossen wurden, sind in der Statistik nicht mehr enthalten. Noch offene Schwachstellen werden dagegen stets aufgeführt, auch wenn deren erstes Auftreten schon vor dem angegebenen Datum liegt.

Produktname
Alle Werte einer produktbezogenen Tabellenzeile gelten für das in der Spalte „Produktname“ angegebene Produkt. In jeder Zeile können dabei sowohl Werte für ein Einzelprodukt als auch für eine ganze Produktfamilie angegeben sein.

Sofern nicht explizit anders angegeben, werden in jedem Fall alle aktuellen Versionen des Produkts für die Ermittlung der Zahlenwerte herangezogen.

Geschlossene Schwachstellen
Neben den sicherheitsrelevanten „offenen Schwachstellen“ wird in jeder Produktzeile auch die Anzahl der bereits „geschlossenen Schwachstellen“ angegeben. Geschlossene Schwachstellen haben keinerlei Auswirkung auf die BSI-Bewertung, die Angabe erfolgt lediglich zu informativen Zwecken. Eine Schwachstelle gilt als geschlossen, wenn durch den Hersteller oder einen autorisierten Dritten ein offizieller und für die Anwender verfügbarer Patch zur Beseitigung der Schwachstelle veröffentlicht wurde. Die hier angegebenen Zahlenwerte beziehen sich dabei ausschließlich auf den genannten Auswertungszeitraum, welcher in der Regel das zurückliegende Jahr umfasst. Durch diese zeitliche Beschränkung sind hier bei Aktualisierungen auch sinkende Zahlenwerte möglich.

Offene Schwachstellen
Schwachstellen, die noch nicht durch Patches der Hersteller behoben werden können und entsprechend der verwendeten CVSS-Metrik als mindestens „geringfügig-kritisch“ einzustufen sind, werden als „offene Schwachstellen“ aufgeführt. Insofern werden offene Schwachstellen, die gemäß der CVSS-Metrik als „nicht kritisch“ bewertet werden, im Rahmen der Schwachstellenampel nicht unter „offenen Schwachstellen“ gezählt oder in einer anderen Form berücksichtigt. Die zugrunde liegende Metrik zur Einordnung von Schwachstellen in die Kategorie „davon kritisch“ wird unter „Maßstab zur Berechnung des Schweregrades einer Lücke“ in einem eigenen Kapitel beschrieben.

BSI-Bewertung
Die BSI-Bewertung überführt die Zahlenwerte der „offenen Schwachstellen“ anhand einer einfachen Systematik in eine Einschätzung des Schweregrades bzw. der daraus resultierenden möglichen Auswirkungen. Die Anzahl der „geschlossenen Schwachstellen“ wird für diese Bewertung nicht berücksichtigt.

Zur Visualisierung dieses Schweregrades bedient sich die BSI-Bewertung einer Ampeldarstellung in den drei Farben „grün“, „gelb“ und „rot“.

Anhand des oben gezeigten Beispiels (*Tabelle 2*) lässt sich das Bewertungsschema folgendermaßen erklären:

Beispiel 1: *Das in Zeile 3 aufgeführte Produkt „Produkt 1“ ist von insgesamt einer offenen Schwachstelle betroffen. Diese Schwachstelle wurde entsprechend der unter „Maßstab zur Berechnung des Schweregrades einer Lücke“ erläuterten Metrik als „kritisch“ eingestuft. Eine solche Schwachstelle bietet einem Angreifer oder einer Schadsoftware oft Erfolg versprechende, relativ einfach auszunutzende Angriffsvektoren. Die Schwachstelle kann beispielsweise zur kompletten Übernahme des Systems durch einen Angreifer führen, sodass ein hohes Schadenspotenzial besteht. Sobald eine offene kritische Schwachstelle vorliegt, gilt für die Bewertung bereits die Ampelfarbe „rot“. Die Anzahl weiterer kritischer oder nicht-kritischer Schwachstellen hat keinen weiteren Einfluss auf die Ampelfarbe.*

Beispiel 2: *Die Produktreihe „Produktfamilie 2“ weist keine offenen kritischen Schwachstellen auf, hat aber dennoch sieben entsprechend der Metrik nicht zu vernachlässigende offene Schwachstellen. Solche Schwachstellen sind schwerer ausnutzbar oder bergen ein vergleichsweise geringeres Schadenspotenzial. Sobald eine, entsprechend der Metrik unter „Maßstab zur Berechnung des Schweregrades einer Lücke“, als „geringfügig-kritische“ eingestufte Schwachstelle vorliegt, gilt für die Bewertung die Ampelfarbe „gelb“. Diese Bewertung gilt solange nicht gleichzeitig mindestens eine kritische Schwachstelle existiert. Die Anzahl der vorhandenen Schwachstellen hat keinen weiteren Einfluss auf die Ampelfarbe.*

Beispiel 3: *Für das Produkt „Produkt 3" sind derzeit keine offenen Schwachstellen bekannt. Das Produkt wird daher mit der Ampelfarbe „grün" bewertet. Diese Bewertung erhalten nur Produkte für die entweder überhaupt keine offenen oder weder „kritische" noch „geringfügig kritische" offene Schwachstellen vorliegen.*

In Kurzform lässt sich das Bewertungsschema anhand der **offenen** Schwachstellen also wie folgt zusammenfassen:

- **rot** bei einer beliebigen Anzahl von offenen Schwachstellen mit mindestens einer „kritischen" (CVSS ≥ 7.0) Schwachstelle
- **gelb** bei einer beliebigen Anzahl von „geringfügig-kritischen" (CVSS zwischen 4.0 und 6.9) offenen Schwachstellen, bei gleichzeitig keiner „kritischen" offenen Schwachstelle
- **grün** wenn für ein Produkt weder „kritische" noch „geringfügig kritische" offene Schwachstellen vorliegen

Gesamtbewertung offener Schwachstellen

Für die herstellerbezogene Gesamtbewertung wird das oben beschriebene Kriterium der BSI-Bewertung auf die Summe aller offenen Schwachstellen angewandt. Die Gesamtbewertung ist damit ein Indikator für das Vorliegen von (kritischen) Schwachstellen in einem oder mehreren beliebigen der aufgeführten Produkte des jeweiligen Herstellers.

Beispiel: *Der Hersteller im Beispiel (Tabelle 2) ist von insgesamt acht Schwachstellen in seinen Produkten betroffen, wovon eine als kritisch eingestuft wurde. Damit ergibt sich für den Hersteller die Gesamtbewertung „rot". Ein Ausgleich durch die gelbe bzw. grüne Bewertung der beiden anderen Produkte ist nicht möglich. Die Gesamtbewertung gibt demnach immer die schlechteste Bewertung aller betrachteten Produkte wieder.*

Eine Vergleichbarkeit zwischen den einzelnen Herstellern ist durch diese Form der Bewertung im Allgemeinen nicht möglich und ist auch nicht Ziel dieser Betrachtung.

Links zu Sicherheitshinweisen der Hersteller

Die in der Schwachstellenampel vertretenen Hersteller bieten in ihren eigenen Internetangeboten meist ausführliche Informationen zu bekannten Schwachstellen und zu deren Behebung durch Patches oder andere Maßnahmen.

Aktualisierung der Schwachstellenampel

Die Schwachstellenampel wird regelmäßig aktualisiert. Die Termine der Aktualisierungen orientieren sich dabei hauptsächlich an den „Patchdays" der Hersteller. Aktualisierungen bei neuen Schwachstellenmeldungen und außerplanmäßig veröffentlichten Patches werden nach Möglichkeit ebenfalls rasch vorgenommen. Verzögerungen bei der Aktualisierung können jedoch nicht ausgeschlossen werden. Sämtliche Werte und Bewertungen der Schwachstellenampel beziehen sich stets auf den jeweils angegebenen Aktualisierungsstand.

Metriken zur Beschreibung einer Sicherheitslücke

Zur Beurteilung der Schwachstellen stützt sich die Schwachstellenampel auf das Common Vulnerability Scoring System (CVSS v2). Bei diesem offenen System handelt es sich um einen Industriestandard, der den Schweregrad von Sicherheitslücken aus verschiedenen Perspektiven betrachtet. Diese Perspektiven spiegeln sich in Metriken wider.

Die Metriken sind untergliedert in Basis-Metriken, zeitgebundene Metriken und Umgebungs-Metriken. In die Bewertung der Sicherheitslücken innerhalb der Schwachstellenampel fließen lediglich die Basis-Metriken ein. Lediglich die Einbeziehung dieser Basis-Metriken liefert ein unabhängiges Maß für den Schweregrad einer Schwachstelle.

Basis-Metriken

Die Werte der Basis-Metriken sollen aufzeigen, wie einfach bzw. aufwändig ein Angriff auf eine bestimmte Sicherheitslücke ist. Zudem soll der mögliche, potenzielle Schaden des Opfers bei einem Angriff angegeben werden können. Die Auswirkungen eines Angriffs auf einen der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit des Opfersystems werden ebenfalls berücksichtigt. Die Basis-Metriken werden formal wie folgt dargestellt:

```
AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
```

Die Bedeutung der einzelnen Vektoren und Werte in der oben dargestellten Form kann Tabelle 2 entnommen werden.

Vektor	Mögliche Werte	Erläuterung
AV = Access Vector	L = Local	Das Ausnutzen der Schwachstelle ist nur per lokalem Zugriff möglich (d. h. physikalischer Zugriff oder über einen lokalen Shell-Account, z. B. Firewire/USB DMA Attacken).
	A = Adjacent Network	Das Ausnutzen der Schwachstelle ist nur über ein Netzwerk möglich, welches sich z. B. in derselben Domäne befindet. Der Angriff erfolgt hier z. B. im lokalen IP-Subnetz oder im lokalen Ethernet-Segment.
	N = Network	Eine Schwachstelle kann über ein anderes Netzwerk oder das Internet ausgenutzt werden, z. B. über ein RPC Buffer Overflow.
AC = Access Complexity	H = High	Es existieren ganz spezielle Zugriffsbedingungen, die in der Praxis selten vorkommen, um die Sicherheitslücke auszunutzen.
	M = Medium	Es existieren wenig spezielle Zugriffsbedingungen, die in der Praxis durchaus vorkommen, um die Sicherheitslücke auszunutzen.
	L = Low	Es existieren keine Zugriffsbedingungen oder Umstände, um die Sicherheitslücke auszunutzen.
Au = Authentication	M = Multiple	Zwei oder mehr Authentisierungsvorgänge sind nötig, um Zugriff auf das System zu erhalten und die Schwachstelle auszunutzen.
	S = Single	Ein Authentisierungsvorgang ist nötig, um Zugriff auf das System zu erhalten und die Schwachstelle auszunutzen.
	N = None	Eine Authentisierung ist nicht notwendig, um Zugriff auf das System zu erhalten und die Schwachstelle auszunutzen.
C = Confidentiality Impact	N = None	Es gibt keine Auswirkung auf die Vertraulichkeit des Systems.
	P = Partial	Entstehung erheblicher Informationsverluste. Lesender Zugriff zu einigen Systemdateien ist möglich.
	C = Complete	Lesender Zugriff ist auf alle Systemdateien möglich.
I = Integrity Impact	N = None	Es bestehen keine Auswirkungen auf die Integrität des Systems.
	P = Partial	Änderungen einiger Systemdateien oder Informationen ist möglich. Der Angreifer hat aber nicht die Kontrolle, welche Systemdateien modifiziert werden können.
	C = Complete	Komplette Kompromittierung des Systems, kompletter Verlust des Systemschutzes.
A = Availibility Impact	N = None	Es existiert keine Auswirkung auf die Verfügbarkeit des Systems.
	P = Partial	Es besteht eine verringerte Performance oder Unterbrechungen in der Verfügbarkeit des Systems.
	C = Complete	Das System ist nicht mehr erreichbar.

Tabelle 2: Auflistung der Basis-Metriken, Quelle: http://www.first.org/cvss/cvss-guide.pdf

Weitere Metriken

Die zeitgebundenen Metriken sollen skalieren, wie sich eine Bedrohung ausgehend von der Entdeckung einer Schwachstelle mit der Zeit ändert. Dabei stellt sich die Frage, ob es sich bei einer Schwachstelle um einen theoretischen Angriff, einen POC (Proof of Concept) handelt, ob der Softwarehersteller schon mit einem Patch oder einem Hotfix reagiert hat, und wie vertrauenswürdig die Quellen der Schwachstellenmeldung sind.

Bei den Umgebungs-Metriken wird die komplette Umgebung innerhalb eines Unternehmens oder einer Behörde betrachtet. Dabei muss geklärt werden welche Schutzbedürfnisse für Daten und Systeme existieren.

Diese Metriken sind optional und gehen nicht in die Gewichtung der Schwachstellenampel mit ein. Allerdings ändert sich der Zustand der Schwachstellenampel, sobald ein Patch oder Hotfix verfügbar ist: Sobald alle kritischen oder geringfügig kritischen Schwachstellen geschlossen wurden, zeigt die Schwachstellenampel grün. Weitere Informationen zu den Metriken können auf den Internetseiten des „Forum for Incident Response and Security Teams“ (http://www.first.org/cvss/cvss-guide.html) nachgelesen werden.

Maßstab zur Berechnung des Schweregrades einer Lücke

Aus den oben aufgeführten Metriken wird schließlich ein standardisierter Wert zwischen 0 und 10 abgebildet. Dieser Wert führt unmittelbar zur Einordnung einer Schwachstelle als „kritisch“, „geringfügig kritisch“ oder „nicht kritisch“:

- **0.0 – 3.9** = Die Schwachstelle wird als **nicht kritisch** angesehen.
- **4.0 – 6.9** = Die Schwachstelle wird als **geringfügig kritisch** angesehen.
- **7.0 – 10.0** = Die Schwachstelle wird als **kritisch** angesehen.

In der Schwachstellenampel wird nur zwischen „kritischen“ (CVSS $\geq$ 7.0) und „geringfügig-kritischen“ (CVSS 4.0 bis 6.9) Sicherheitslücken unterschieden. Sofern für ein Produkt weder „kritische“ noch „geringfügig kritische“ offene Schwachstellen vorliegen, zeigt die Schwachstellenampel daher grün.

Detailliertere Informationen zur Berechnung solcher Werte aus den Metriken können in der Entwurfsversion der CVSS v2 Berechnungsformeln (http://nvd.nist.gov/cvsseq2.htm) gefunden werden. Die Einordnung von Sicherheitslücken mithilfe der Schwachstellenampel stellt lediglich einen Richtwert für eine allgemein korrekte Einordnung einer Schwachstelle dar. Die Verantwortlichen in den Unternehmen sind gefordert, bekannt gewordene Schwachstellen in Beziehung zu ihren individuellen unternehmerischen Rahmenbedingungen und IT-Infrastrukturen zu setzen und nach eigenen Gegebenheiten (Metriken) zu gewichten und zu bewerten. Unterstützung dabei können Online-Rechner bieten, wie beispielsweise der „CVSSv2 Calculator“ des NIST (http://nvd.nist.gov/cvss.cfm?calculator&version=2) oder der „CVSS Online Calculator, version 2.0“ (http://intellishield.cisco.com/security/alertmanager/cvss).

Nummerierung der Schwachstellen

Jede bestätigte Schwachstelle erhält eine CVE-Nummer (Common Vulnerability and Exposures), durch welche sie eindeutig identifizierbar ist. Mehr Informationen zur Zuweisung und Verwendung von CVE-Nummern sind auf der CVE-Website (http://www.cve.mitre.org) abrufbar. Gelegentlich wird für mehrere Schwachstellen eines Produktes aufgrund ihrer Ähnlichkeit nur eine gemeinsame Nummer vergeben. In der Schwachstellenampel werden diese folglich auch nur als eine Schwachstelle gezählt.