

Threat Update: Sendmail Race Condition

Lukas Feiler, Achim Brock

23. März 2006

Veröffentlichungsdatum d. Sicherheitslücke: 22. März 2006

Betroffene Software: Sendmail vor Version 8.13.6

MITRE CVE-Nummer: CVE-2006-0058

Bugtraq ID: 17192

US-CERT Vulnerability Note: VU#834865

US-CERT Technical Cyber Security Alert: TA06-081A

Inhalt

1. Einleitung
2. Beschaffenheit der Sicherheitslücke
3. Auswirkungen der Sicherheitslücke
4. Strafrechtliche Beurteilung
 - 4a) Verletzung der Vertraulichkeit von E-Mails
 - 4b) Veränderung und Unterdrückung von E-Mails
 - 4c) Störung der Funktionsfähigkeit des gesamten Mail-Servers
 - 4d) Zugangsverschaffung zum Computersystem

1. Einleitung

Sendmail ist der für Unix/Linux-Systeme am häufigsten eingesetzte Mail Transport Agent (MTA). Dieser implementiert die Funktionalität des Versendens und Empfangens von E-Mails mittels SMTP¹. MTAs (auch SMTP-Server genannt) sind für viele Organisationen von höchster Wichtigkeit, da die Vertraulichkeit und Verfügbarkeit der E-Mail-Kommunikation meist als geschäftskritisch eingestuft werden muss.

2. Beschaffenheit der Sicherheitslücke

Es handelt sich um eine Race Condition. Vgl allgemein hierzu *Feiler*, 35 f. Es ist einem Angreifer möglich zwischen dem Aufruf zweier Funktionen² den von Funktion #1 gespeicherten Programm-Status derart zu verändern, dass Funktion #2 beliebige Befehle des Angreifers ausführt. Dies erfordert jedoch, dass Teile eines, als Stack bezeichneten Bereichs des Hauptspeichers überschrieben werden.³

3. Auswirkungen der Sicherheitslücke

Da sendmail idR mit administrativen Rechten⁴ auf eine Unix/Linux-System ausgestattet ist, ermöglicht diese Sicherheitslücke die Kompromittierung des gesamten Betriebssystems. Unabhängig hiervon erlangt der Angreifer jedenfalls ausreichende Berechtigungen um wahlweise

- a) sich von alle ein- und ausgehenden E-Mails Kenntnis zu verschaffen
- b) einzelne E-Mails nach belieben zu verändern oder zu unterdrücken
- c) sendmail gänzlich zu deaktivieren bzw. „herunterzufahren“
- d) sich von sonstigen im Computersystem gespeicherten Daten Kenntnis zu verschaffen

Die nun folgende strafrechtliche Beurteilung ist in diese vier Punkte gegliedert.

¹ spezifiziert in RFC 2821, <ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt>

² setjmp und longjmp; vgl. <http://linuxgazette.net/issue90/raghu.html>

³ vgl. <http://xforce.iss.net/xforce/alerts/id/216>

⁴ d.h. mit root-Rechten; zur Problematik sendmail's monolithischen Designs vgl. *Graff/Van Wyk*, *Secure Coding: Principles and Practices*, 90 ff, O'Reilly, Sebastopol 2003

4. Strafrechtliche Beurteilung

a) Verletzung der Vertraulichkeit von E-Mails

Verschafft sich der Angreifer Kenntnis von ein- bzw. ausgehenden E-Mails kommt eine Strafbarkeit nach §§ 119, 119a, 123 StGB und § 51 DSGVO in Betracht.

Ungeachtet welcher konkreten technischen Mittel sich der Angreifer zur Kenntnisverschaffung der E-Mails bedient, wird es sich hierbei um eine Abhörvorrichtung iSd § 119 StGB handeln, die der Täter auch mit Eventualvorsatz benützt. Da die Klassifizierung einer E-Mail als Gedankenerklärung idR unproblematisch ist und diese im Wege eines Computersystems übertragen wird, ist sofern der Täter diesbezüglich und bezüglich der Kenntnisverschaffung mit Absichtlichkeit handelt eine Strafbarkeit nach § 119 zu bejahen.

Hat der Täter ausnahmsweise nur den Vorsatz sich von E-Mails Kenntnis zu verschaffen, die keine Gedankenerklärung darstellen (z.B. von Programmen automatisch generierte E-Mails die sensitive Daten wie Passwörter enthalten können⁵) scheidet § 119 aus. In diesen Fällen kommt subsidiär eine Strafbarkeit nach § 119a in Betracht, da hier der weite Datenbegriff iSd § 74 Abs 2 verwendet wird. Neben dem Tatbildvorsatz muss jedoch ein erweiterter Vorsatz in Form der Absichtlichkeit vorliegen. Denn der Täter muss mit Spionage- Verwendungs- und Gewinn- bzw. Schädigungsabsicht handeln.⁶ Auf Grund dieser starken Einschränkung des Tatbestandes wird eine Strafbarkeit nach § 119a idR zu verneinen sein.

Wird ein, in den E-Mails enthaltenes Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, so besteht eine Strafbarkeit nach § 123 StGB.

Nach § 51 DSGVO tritt eine Strafbarkeit erst dann ein, wenn der Täter die so erlangten personenbezogene Daten iSd § 4 Z 1 DSGVO benützt, zugänglich macht oder veröffentlicht. Der subjektive Tatbestand erfordert neben dem Tatbildvorsatz einen erweiterten Vorsatz in Form der Absichtlichkeit sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen.

b) Veränderung und Unterdrückung von E-Mails

Hierbei ist an eine Strafbarkeit wegen Datenbeschädigung gem § 126a StGB zu denken. Da die Wiederherstellung der veränderten bzw. unterdrückten (d.h. gelöschten) E-Mails meist einen erheblichen Aufwand verursachen, ist eine vorsätzliche Veränderung oder Unterdrückung von E-Mails nach § 126a strafbar.

c) Störung der Funktionsfähigkeit des gesamten Mail-Servers

Führt der Angreifer vorsätzlich einen Denial of Service Attack aus, indem er sendmail bzw. das gesamte Betriebssystem herunterfährt, liegt eine schwere Störung der Funktionsfähigkeit eines Computersystems vor, weshalb eine Strafbarkeit nach § 126b StGB zu bejahen ist.

d) Zugangsverschaffung zum Computersystem

Bereits im Stadium der Zugangsverschaffung zum Mail-Server kommt eine Strafbarkeit nach § 118a StGB in Betracht. Der objektive Tatbestand erfordert, dass der Täter sich Zugang zu dem Computersystem verschafft, indem er eine Sicherheitsvorkehrung im Computersystem verletzt. Die Ausnützung einer Race Condition stellt für sich keine Verletzung iSd § 118a

⁵ vgl. Feiler, 20

⁶ vgl. Feiler, 21

StGB dar.⁷ Im vorliegenden Fall erfolgt die Zugangsverschaffung jedoch noch nicht unmittelbar durch die Ausnutzung der Race Condition sondern erst durch die Überschreibung eines, als Stack bezeichneten Bereichs des Hauptspeichers. Da dieser unmittelbar den logischen Programmfluss determiniert, ist er als Teil des Programms zu beurteilen. Da das Programm jedoch die Sicherheitsvorkehrung „Least Privilege“⁸ implementiert, stellt die Beeinträchtigung der Datensubstanz des Stacks als Teil des Programms eine Verletzung einer Sicherheitsvorkehrung dar.⁹

Quellen:

<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-0058>

<http://www.securityfocus.com/bid/17192/info>

<http://www.kb.cert.org/vuls/id/834865>

<http://www.us-cert.gov/cas/techalerts/TA06-081A.html>

<http://www.sendmail.com/company/advisory/>

<http://xforce.iss.net/xforce/alerts/id/216>

Klensin, RFC 2821, Simple Mail Transfer Protocol, 2001, <ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt>

Feiler, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 2006

⁷ vgl. *Feiler*, 35 ff, beispielsweise CVE-2004-0594, ausführlich beschrieben in *Feiler*, 45

⁸ *Garfinkel/Spafford/Schwartz*, Practical Unix & Internet Security³, 235, O'Reilly, Sebastopol 2003; *Feiler*, 14 f

⁹ *Feiler*, 26 f