Sendmail의 원격버퍼오버플로우 취약점 대응 방법

(Ver. 1.5)

2003.03.06(목)
last update 2003.03.15(금)

연구원 윤승노 (snyoon@certcc.or.kr)
연구원 이동련 (ryuni@certcc.or.kr)
연구원 류성철 (ryusc@certcc.or.kr)

본 문서는 2003년 3월 4일 발표된 sendmail의 원격버퍼오버플로우 취약점에 대한 대응 방법에 대하여 CERTCC-KR 내 시험망에서 테스트 한 결과를 토대로 작성되었다. 현재 Ver.1.5에서는 SUN 운영체제에 관한 자료와 RedHat 리눅스의 바이너리 패치적용 방법만을 수록하고 있으며, 추후 지속적으로 업데이트 할 예정이다.

1. SUN 시스템

가. 패치 적용방법

SUN 마이크로시스템즈에서는 해당 Sendmail 취약점에 대하여 바이너리 패치파일을 적용하는 방법과 소스코드의 수정 후 Sendmail 파일을 대체하는 두 가지 방법으로 적용할 수 있다. 그러나 설정파일 변경등의 영향을 최소화하기 위하여 소스코드 패치방법을 권장한다. 또한 두 가지 패치방법 모두 패치과정 중에 sendmail 서비스를 중지하여야 하므로, 실제 운영중인 메일서버의 경우 이로 인한 영향을 최소화하여야 한다.

기본적으로 패치를 적용하기 이전에 자신이 사용하고 있는 sendmail의 버전을 확인하도록 한다. 버전을 확인하기 위해 sendmail이 기본적으로 사용하는 tcp/25 포트에 접속을 시도하여 나타나는 메시지를 참고한다.

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 NibbleTest ESMTP Sendmail 8.11.6/8.11.6; Wed, 5 Mar 2003 20:14:51
+0900 (KST)
```

위에서는 본 문서에서 사용하는 시험환경의 sendmail이 버전 8.11.6임을 나타내고 있다.

1) 바이너리 패치 적용

가) 패치파일 다운로드

썬 마이크로시스템즈에서 제공하는 패치 파일은 바이너리 형태로 제공되며, 운영체제의 버전에 따라 8가지 형태가 있다. 다음의 표에서는 각 운영체제 버전별 패치번호(Patch-ID)를 나타낸다.

	Sparc 계열	x86 계열	비고
Solaris 2.6 (SunOS 5.6)	105395-08	105396-08	
Solaris 7 (SunOS 5.7)	107684-08	107685-08	
Solaris 8 (SunOS 5.8)	110615-08	110616-08	
Solaris 9 (SunOS 5.9)	113575-03	114137-02	

각각의 패치는 sunsolve홈페이지(http://sunsolve.sun.com)에서 다운로드 받을 수 있다.

나) 준비과정

패치를 적용시키기 위해서는 패치를 설치하는 동안 일시적으로 sendmail 서비스를 중지하여야 한다. 현재 sendmail 서비스의 작동여부를 확인하기 위해서는 다음의 명령어를 실행시켜 확인할 수 있다.

```
$ /usr/bin/ps -ef |grep sendmail
```

sendmail이 실행되고 있는 경우에는 다음과 같이 해당 프로세스 번호 및 구동시간 등의 정보가 나타나게 된다.

```
root   978     1   0 13:30:51 pts/1     0:00 /usr/lib/sendmail -bd -q15m
```

sendmail이 실행되고 있지 않은 상태라면 바로 패치를 적용할 수 있으며, sendmail이 구동되고 있는 상태라면 다음의 명령어를 통해 sendmail 서비스를 중지시켜야 한다.

```
# /etc/init.d/sendmail stop
```

다) 기존 파일 백업하기

패치를 적용시키는 경우 기존의 설정값이 변경(overwrite)되기 때문에 기존의 설정파일들을 백업할 필요가 있다. /etc/mail 디렉토리 하단의 설정파일들과 sendmail 실행파일 (일반적으로, /usr/lib/sendmail 또는 /usr/sbin/sendmail)을 백업한다. 정확한 설정파일 목록을 알지 못하는 경우에는 /etc/mail 디렉토리 전체와 실행파일을 백업 받아두도록 한다.

라) 패치 설치하기

먼저 다운로드 받은 파일의 압축을 해제한다.

```
# gzip -d 107684-08.tar.gz
# tar -xvf 107684-08.tar
```

※ 본 문서에서는 Solaris 7 sparc 버전을 기준으로 기술한 것으로, 각 사용자는 각 운영체제에 해당하는 패치파일 명을 적어야 한다.

patchadd 명령어를 이용하여 압축이 해제된 디렉토리의 상위 디렉토리에서 명령을 실행시키거나, 다른 디렉토리에 압축을 해제한 경우 절대경로를 적어 패치를 적용시킨다.

```
# patchadd 107684-08
또는
# patchadd /var/spool/patch/107684-08
```

※ patch 적용을 취소하고자 하는 경우에는 patchadd 대신 patchrm 명령어를 사용하면 된다.

2) 소스 코드 패치 적용

가) 다운로드

소스코드 패치버전은 2003.03.06 현재 아래와 같이 4가지 버전에 대해 제공되며, 패치파일은 http://www.sendmail.org/patchcr.html 에서 다운 받을 수 있다.

- sendmail 8.12.X : sendmail.8.12.security.cr.patch
- sendmail 8.11.X : sendmail.8.11.6.security.cr.patch
- sendmail 8.10.X : sendmail.8.11.6.security.cr.patch
- sendmail 8.9.X : sendmail.8.9.3.security.cr.patch

※ sendmail 8.10.X 버전과 8.11.X 버전에는 동일하게 8.11.6패치를 적용한다.

나) 준비과정

바이너리 패치과정과 동일하게 ps 명령어를 이용하여 sendmail 서비스 구동여부를 확인하고, 구동 중인 서비스를 중지시킨다.

※「1) 바이너리 패치 적용」의「나) 준비과정」참조

다) 기존 파일 백업하기

기본적으로 소스코드 패치는 실행파일만을 재컴파일하여 복사하는 과정으로, 설정파일 및 기존파일의 백업이 필요하지 않지만, 만약의 경우를 대비하여 백업하여 둘 것을 권장한다.

※「1) 바이너리 패치 적용」의「다) 기존 파일 백업하기」참조

라) 패치 설치하기

먼저 자신의 시스템에 설치된 sendmail의 버전에 해당하는 파일의 압축을 해제한다.

```
# gzip -d sendmail.8.11.6.security.cr.patch.gz
```

※ 본 문서에서는 Solaris 7 sparc 버전환경에서의 sendmail 8.11.6을 기준으로 기술한 것으로, 각 사용자는 각 운영체제 및 sendmail 버전에 해당하는 패치파일 명을 적어야 한다.

재컴파일을 하기 위해 최초 설치를 실행한 sendmail 디렉토리로 이동한다. 해당 디렉토리를 찾을 수 없거나, 최초 설치 디렉토리를 삭제한 경우에는 현재 운영중인 버전의 sendmail 프로그램을 다시 다운(ftp://ftp.sendmail.org/pub/sendmail) 받는다.

해당 sendmail의 headers.c 소스코드가 존재하는 디렉토리(일반적으로 sendmail 하위디렉토리 중 src 디렉토리 또는 obj.XXX 디렉토리에 존재)로 이동한 후 다음과 같이 패치를 적용한다.

```
# patch -p0 < /PATH/TO/sendmail.8.11.6.security.cr.patch
```

※ 패치가 정상적으로 적용된 경우 성공 메시지가 출력된다.

패치를 적용 한 후에는 재컴파일하여 바이너리 파일을 생성한다. 일반적으로 컴파일을 실행하기 위해서 make를 사용하지만 sendmail의 경우 Build라는 독자적인 컴파일 도구를 제공한다. 다음과 같이 sendmail디렉토리에서 sh Build를 실행한다.

```
# sh ./Build
```

재컴파일이 완료되면 새로운 바이너리 파일(sendmail)이 정상적으로 생성되었는지를 확인한 후 해당 디렉토리의 하위디렉토리 중 makemap이라는 디렉토리로 이동하여 make install을 실행하여 작업을 마무리한다.

```
# cd makemap
# make install
```

마지막으로 새롭게 생성된 sendmail 바이너리 파일을 실행위치에 복사한다. 실행위치는 일반적으로 /usr/lib 또는 /usr/sbin 이다.

```
# cp ./sendmail /usr/lib/
```

나. 패치 적용 확인 방법

패치가 모두 완료된 경우, 다음과 같이 sendmail을 다시 시작한다.

```
# /etc/init.d/sendmail start
```

sendmail이 정상적으로 동작하는지 여부를 확인하기 위해서는 세가지의 방법이 있다. 첫째, 앞에서 살펴본 바와 같이 ps 명령어를 이용하여 프로세스가 정상적으로 동작 중인지를 확인한다. 둘째, 다음과 같이 smtp포트(일반적으로 tcp/25)에 접속을 하여 정상동작을 확인할 수 있다.

```
 # telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 NibbleTest ESMTP Sendmail 8.11.6/8.11.6; Wed, 5 Mar 2003 20:14:51
+0900 (KST)
```

접속을 시도한 경우 위에서와 같이 이탤릭체로 표시된 부분과 유사한 메시지가 나타난다면 정상동작하는 것이다.

셋째, 이상의 확인 방법을 통해 정상적 작동을 확인한 경우, 마지막으로 메일 전달이 정상적으로 이루어지는지를 확인한다.

```
# /usr/lib/sendmail -v userid
 test
 testmail sending

 .

 userid... Connecting to local...
 userid... Sent
```

※ *userid* 부분에는 해당 시스템에 등록된 사용자 아이디를 적는다.

※ 이탤릭체로 표시된 부분은 시스템에서 출력하는 메시지이다.

정상 작동이 확인된 이후, 패치가 정상적으로 적용되었는지를 확인하는 방법은 다음과 같다.

먼저, sendmail 실행파일이 위치한 디렉토리를 찾아간다. 일반적으로 sendmail 실행파일은 /usr/lib/ 또는 /usr/sbin/ 디렉토리에 위치하게 된다. sendmail 바이너리 파일이 존재하는지를 확인한 후 strings 명령어를 이용하여 다음과 같은 문자열을 확인한다. 이탤릭체로 표시된 해당 문자열이 나타난다면 정상적으로 패치가 적용된 것이고, 나타나지 않는 경우 다시 패치를 적용한다.

```
/usr/lib> strings sendmail | grep 'Dropped invalid comments from header
          address'

Dropped invalid comments from header address
```

이상의 sendmail 서비스 동작여부 확인 및 패치성공 여부를 수동으로 확인하기 어려운 경우, CERTCC-KR에서 제공하는 쉘 스크립트를 이용하면 된다. 쉘 스크립트를 다운받을 수 있는 위치와 사용방법은 다음과 같다.

- 다운로드 위치 : http://www.certcc.or.kr/paper/tr2003/sendmail_check.sh

다운로드 받은 점검파일을 임의의 디렉토리에 복사한 후, 퍼미션에 실행권한이 부여되어 있는지를 확인한다. 실행권한이 없는 경우 다음과 같이 실행권한을 부여한다.

```
# chmod +x ./sendmail_check.sh
```

모든 준비가 완료되었으면 해당 스크립트를 실행한다. 해당 스크립트에서는 sendmail 실행파일 검색작업이 포함되어 있어, 시스템에 따라 몇 분이 소요되는 경우도 있다.

```
# ./sendmail_check.sh
Starting find sendmail. Please Wait.....
OK. Safe Sendmail
```

위에서 보는 바와 같이 '*OK. Safe Sendmai*' 메세지가 나타난 경우 패치가 정상적으로 적용되었음을 의미한다. '**** Alert! Sendmail Patch needed! ****' 메시지가 나타난 경우에는 패치를 재적용하여야 하며, '**** Can't find sendmail program! ****'메세지가 출력되는 경우 sendmail프로그램이 설치되어 있지 않거나, sendmail 실행파일을 찾을 수 없는 경우이다.

2. RedHat 시스템

가. 패치 적용방법

RedHat 리눅스 시스템에서는 해당 Sendmail 취약점에 대하여 바이너리 패치파일을 적용하는 방법과 소스코드의 수정 후 Sendmail 파일을 대체하는 두 가지 방법으로 적용할 수 있으며 본 문서에서는 현재 바이너리 패치파일 적용방법에 대해서만 소개한다.

기본적으로 패치를 적용하기 이전에 자신이 사용하고 있는 RedHat 버전을 확인하도록 한다. 버전을 확인하는 방법은 다음과 같다.

```
# cat /etc/redhat-release
Red Hat Linux release 7.2 (Enigma)
```

위에서는 본 문서에서 사용하는 시험환경의 RedHat 버전이 7.2임을 나타낸다.

1) 바이너리 패치 적용

RedHat 시스템에서 바이너리 패치를 적용하는 방법은 기본적으로 SUN 시스템에서 사용하는 방법과 동일하나 구체적인 명령어에서 다소 차이가 있다.

가) 패치파일 다운로드

바이너리 패치버전은 2003.03.14 현재 아래와 같이 6가지 버전에 대해 제공되며 패치파일은 http://rhn.redhat.com/errata/RHSA-2003-073.html에서 다운 받을 수 있다.

버전	파일명
Red Hat Linux 6.2	sendmail-8.11.6-23.62.i386.rpm
Red Hat Linux 7.0	sendmail-8.11.6-23.70.i386.rpm
Red Hat Linux 7.1	sendmail-8.11.6-23.71.i386.rpm
Red Hat Linux 7.2	sendmail-8.11.6-23.72.i386.rpm
Red Hat Linux 7.3	sendmail-8.11.6-23.73.i386.rpm
Red Hat Linux 8.0	sendmail-8.12.8-1.80.i386.rpm

나) 준비과정

패치를 적용시키기 위해서는 패치를 설치하는 동안 일시적으로 sendmail 서비스를 중지하여야 한다. 현재 sendmail 서비스의 작동여부를 확인하기 위해서는 다음의 명령어를 실행시켜 확인할 수 있다.

```
# ps -ef |grep sendmail
```

sendmail이 실행되고 있는 경우에는 다음과 같이 해당 프로세스 번호 및 구동시간 등의 정보가 나타나게 된다.

```
root    955      1   0 18:01:? 00:00:00 sendmail : accepting connections
```

sendmail이 실행되고 있지 않은 상태라면 바로 패치를 적용할 수 있으며, sendmail이 구동되고 있는 상태라면 다음의 명령어를 통해 sendmail 서비스를 중지시켜야 한다.

```
# /etc/rc.d/init.d/sendmail stop
```

다) 기존 파일 백업하기

패치를 적용시키는 경우 기존의 설정값이 변경(overwrite)되기 때문에 기존의 설정파일들을 백업할 필요가 있다. /etc/mail 디렉토리 하단의 설정파일들, /etc/sendmail.cf와 sendmail 실행파일 (일반적으로, /usr/lib/sendmail 또는 /usr/sbin/sendmail)을 백업한다. 정확한 설정파일 목록을 알지 못하는 경우에는 /etc/mail 디렉토리 전체와 /etc/sendmail.cf, 실행파일을 백업 받아두도록 한다.

라) 패치 설치하기

.rpm 파일을 다운로드 받은 디렉토리로 이동한 후 다음과 같이 rpm 명령어를 사용하여 설치한다.

```
# rpm -Fvh sendmail-8.11.6-23.72.i386.rpm
```

※ 본 문서에서는 RedHat 7.2 버전을 기준으로 기술한 것으로, 각 사용자는 각 운영체제에 해당하는 패치파일 명을 적어야 한다.

패치 설치가 완료되면 기존에 사용하던 설정파일들이 변경되므로 위에서 백업 받은 설정파일들(/etc/mail 디렉토리 하단의 설정파일들, /etc/sendmail.cf)로 대체하여야 정상적인 메일서버의 운영이 가능하다.

나. 패치 적용 확인 방법

패치가 모두 완료된 경우, 다음과 같이 sendmail을 다시 시작한다.

```
# /etc/rc.d/init.d/sendmail start
```

sendmail이 정상적으로 동작하는지 여부를 확인하기 위해서는 SUN 시스템에서와 마찬가지로 세가지의 방법이 있다. 첫째, ps 명령어를 이용하여 프로세스가 정상적으로 동작 중인지를 확인하는 방법과 smtp포트(일반적으로 tcp/25)에 접속하여 정상동작을 확인할 수 있다. 셋째, 이상의 확인 방법을 통해 정상적 작동을 확인한 경우, 마지막으로 메일 전달이 정상적으로 이루어지는지를 확인한다.

※「1.SUN 시스템」의「나. 패치 적용 확인 방법」참조

이상의 sendmail 서비스 동작여부 확인 및 패치성공 여부를 수동으로 확인하기 어려운 경우, CERTCC-KR에서 제공하는 쉘 스크립트를 이용하면 된다. 쉘 스크립트를 다운받을 수 있는 위치와 사용방법은 SUN 시스템과 동일하다.

- 다운로드 위치 : http://www.certcc.or.kr/paper/tr2003/sendmail_check.sh

※「1.SUN 시스템」의「나. 패치 적용 확인 방법」참조