Red Hat Enterprise Linux 8

보안 업데이트 관리 및 모니터링

RHEL 8 시스템 보안을 업데이트하여 공격자가 알려진 취약점을 악용하지 못하도록

Last Updated: 2023-09-19

Red Hat Enterprise Linux 8 보안 업데이트 관리 및 모니터링

RHEL 8 시스템 보안을 업데이트하여 공격자가 알려진 취약점을 악용하지 못하도록

법적 공지

초록

보안 업데이트를 설치하고 업데이트에 대한 추가 세부 정보를 표시하여 새로 발견된 위협 및 취약점으로부터 Red Hat Enterprise Linux 시스템을 보호하는 방법을 알아보십시오.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서 및 웹 속성에서 문제가 있는 언어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

RED HAT 문서에 관한 피드백 제공

문서에 대한 피드백에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

특정 문구에 대한 의견 제출

1. **Multi-page HTML** 형식으로 설명서를 보고 페이지가 완전히 로드된 후 오른쪽 상단 모서리에 **피드백** 버튼이 표시되는지 확인합니다.
2. 커서를 사용하여 주석 처리할 텍스트 부분을 강조 표시합니다.
3. 강조 표시된 텍스트 옆에 표시되는 **피드백 추가** 버튼을 클릭합니다.
4. 의견을 추가하고 **제출** 을 클릭합니다.

Jira를 통해 피드백 제출 (등록 필요)

1. Jira 웹 사이트에 로그인합니다.
2. 상단 탐색 모음에서 **생성** 을 클릭합니다.
3. **Summary** (요약) 필드에 설명 제목을 입력합니다.
4. **Description** (설명) 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

1장. 보안 업데이트 확인

현재와 미래의 위협으로부터 기업 시스템을 안전하게 보호하려면 정기적인 보안 업데이트가 필요합니다. Red Hat 제품 보안은 엔터프라이즈 솔루션을 배포하고 유지하는 데 필요한 지침을 제공합니다.

1.1. 보안 공지란 무엇입니까?

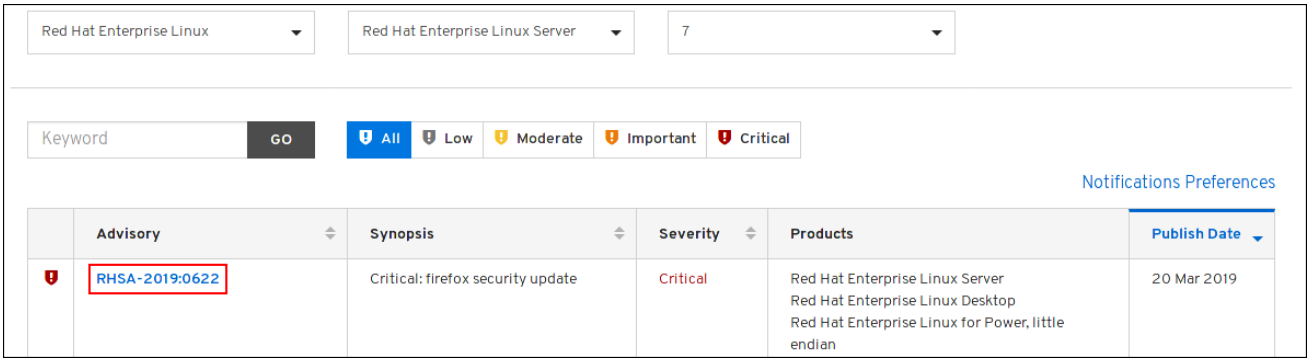
RHSA(Red Hat Security Advisories)에서는 Red Hat 제품 및 서비스에서 수정되는 보안 결함에 대한 정보를 문서화합니다.

각 RHSA에는 다음 정보가 포함됩니다.

- 심각도
- 유형 및 상태
- 영향을 받는 제품
- 수정된 문제 요약
- 문제에 대한 티켓에 링크합니다. 모든 티켓이 공개되는 것은 아니라는 점에 유의하십시오.
- CVE(Common Vulnerabilities and Exposures) 수 및 공격 복잡성과 같은 추가 세부 정보가 포함된 링크.

Red Hat 고객 포털은 Red Hat에서 발행한 Red Hat 보안 공지 목록을 제공합니다. Red Hat 보안 공지 목록에서 권고 ID로 이동하여 특정 권고에 대한 세부 정보를 표시할 수 있습니다.

그림 1.1. 보안 권고 목록



선택적으로 특정 제품, 변형, 버전 및 아키텍처에 따라 결과를 필터링할 수도 있습니다. 예를 들어 Red Hat Enterprise Linux 8에 대한 공지만 표시하려면 다음 필터를 설정할 수 있습니다.

- 제품: Red Hat Enterprise Linux
- 변형: 모든 변형
- 버전: 8
- 선택적으로 8.2와 같은 마이너 버전을 선택합니다.

추가 리소스

- Red Hat 보안 공지 목록

- Red Hat 보안 공지 분석
- Red Hat Customer Portal

1.2. 호스트에 설치되지 않은 보안 업데이트 표시

yum 유틸리티를 사용하여 시스템에 사용 가능한 모든 보안 업데이트를 나열할 수 있습니다.

사전 요구 사항

- 호스트에 연결된 Red Hat 서브스크립션.

절차

- 호스트에 설치되지 않은 사용 가능한 모든 보안 업데이트를 나열합니다.

```
# yum updateinfo list updates security
...
RHSA-2019:0997 Important/Sec. platform-python-3.6.8-2.el8_0.x86_64
RHSA-2019:0997 Important/Sec. python3-libs-3.6.8-2.el8_0.x86_64
RHSA-2019:0990 Moderate/Sec.  systemd-239-13.el8_0.3.x86_64
...
```

1.3. 호스트에 설치된 보안 업데이트 표시

yum 유틸리티를 사용하여 시스템에 설치된 보안 업데이트를 나열할 수 있습니다.

절차

- 호스트에 설치된 모든 보안 업데이트를 나열합니다.

```
# yum updateinfo list security --installed
...
RHSA-2019:1234 Important/Sec. libssh2-1.8.0-7.module+el8+2833+c7d6d092
RHSA-2019:4567 Important/Sec. python3-libs-3.6.7.1.el8.x86_64
RHSA-2019:8901 Important/Sec. python3-libs-3.6.8-1.el8.x86_64
...
```

단일 패키지의 여러 업데이트가 설치되어 있으면 **yum** 은 패키지에 대한 모든 권고를 나열합니다. 이전 예에서는 시스템 설치 이후 **python3-libs** 패키지에 대한 두 가지 보안 업데이트가 설치되었습니다.

1.4. YUM을 사용하여 특정 권고 표시

yum 유틸리티를 사용하여 업데이트에 사용할 수 있는 특정 권고 정보를 표시할 수 있습니다.

사전 요구 사항

- 호스트에 연결된 Red Hat 서브스크립션.
- 보안 권고 **업데이트 ID** 가 있습니다. 보안 권고 업데이트 식별을 참조하십시오.
- 권고에서 제공한 업데이트는 설치되지 않습니다.

절차

- 특정 권고를 표시합니다.

```
# yum updateinfo info <Update ID>
==============================================================================
  Important: python3 security update
==============================================================================
  Update ID: RHSA-2019:0997
       Type: security
    Updated: 2019-05-07 05:41:52
       Bugs: 1688543 - CVE-2019-9636 python: Information Disclosure due to urlsplit improper
NFKC normalization
       CVEs: CVE-2019-9636
Description: ...
```

Update ID 를 필수 권고로 바꿉니다. 예를 들면 **# yum updateinfo info *<RHSA-2019:0997>*** 입니다.

2장. 보안 업데이트 설치

2.1. 사용 가능한 모든 보안 업데이트 설치

시스템의 보안을 최신 상태로 유지하기 위해 **yum** 유틸리티를 사용하여 현재 사용 가능한 모든 보안 업데이트를 설치할 수 있습니다.

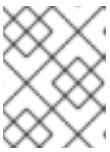
사전 요구 사항

- 호스트에 연결된 Red Hat 서브스크립션.

절차

1. **yum** 유틸리티를 사용하여 보안 업데이트를 설치합니다.

```
# yum update --security
```



참고

security **매개변수** 는 중요합니다. **yum update** 는 버그 수정 및 기능 향상을 포함한 모든 업데이트를 설치합니다.

2. **y**:를 눌러 설치를 확인하고 시작하십시오.

```
...
Transcription Summary
==========================================
Upgrade  ... Packages

Total download size: ... M
Is this ok [y/d/N]: y
```

3. 선택 사항: 업데이트된 패키지를 설치한 후 시스템을 수동으로 다시 시작해야 하는 프로세스를 나열합니다.

```
# yum needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
```

참고

이 명령은 서비스가 아닌 재시작이 필요한 프로세스만 나열합니다. 즉, **systemctl** 유틸리티를 사용하여 나열된 프로세스를 다시 시작할 수 없습니다. 예를 들어 이 프로세스를 소유한 사용자가 로그아웃하면 출력의 **bash** 프로세스가 종료됩니다.

2.2. 특정 권고에서 제공하는 보안 업데이트 설치

특정 업데이트만 설치해야 하는 경우도 있습니다. 예를 들어, 다운타임을 예약하지 않고 특정 서비스를 업데이트할 수 있는 경우 이 서비스에 대해서만 보안 업데이트를 설치하고 나중에 나머지 보안 업데이트를 설치할 수 있습니다.

사전 요구 사항

- 호스트에 연결된 Red Hat 서브스크립션.
- 보안 권고 업데이트 ID가 있습니다. 보안 권고 업데이트 식별을 참조하십시오.

절차

1. 특정 권고를 설치합니다.

```
# yum update --advisory=<Update ID>
```

Update ID 를 필수 권고로 바꿉니다. 예를 들어 **#yum update --advisory= <RHSA-2019:0997>**

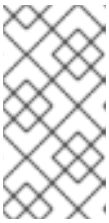
2. **y**:를 눌러 설치를 확인하고 시작하십시오.

```
...
Transaction Summary
==========================================
Upgrade  ... Packages

Total download size: ... M
Is this ok [y/d/N]: y
```

3. 선택 사항: 업데이트된 패키지를 설치한 후 시스템을 수동으로 다시 시작해야 하는 프로세스를 나열합니다.

```
# yum needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
```



참고

이 명령은 서비스가 아닌 재시작이 필요한 프로세스만 나열합니다. 즉, **systemctl** 유틸리티를 사용하여 나열된 모든 프로세스를 다시 시작할 수 없습니다. 예를 들어 이 프로세스를 소유한 사용자가 로그아웃하면 출력의 **bash** 프로세스가 종료됩니다.

2.3. 보안 업데이트 자동 설치

다음 절차에 따라 보안 업데이트로 시스템을 자동으로 업데이트합니다.

사전 요구 사항

- 호스트에 연결된 Red Hat 서브스크립션.

절차

1. yum을 사용하여 dnf-automatic 설치

```
# yum install dnf-automatic
```

2. y를 눌러 설치를 확인하고 시작합니다.

```
...
Transaction Summary
==========================================
Upgrade  ... Packages
Total download size: ... M
Is this ok [y/d/N]: y
```

3. 선택한 텍스트 편집기에서 **/etc/dnf/automatic.conf** 파일을 엽니다. 예를 들면 다음과 같습니다.

```
# vi /etc/dnf/automatic.conf
```

4. **[commands]** 섹션에서 **upgrade_type = security** 옵션을 구성합니다.

```
[commands]
#  What kind of upgrade to perform:
# default                            = all available upgrades
# security                           = only the security upgrades
upgrade_type = security
```

5. **systemd 타이머 장치** 활성화

```
# systemctl enable --now dnf-automatic-install.timer
```

추가 리소스

- **DNF-automatic(8)** 도움말 페이지

2.4. 추가 리소스

- Security Hardening 문서를 통해 워크스테이션과 서버 보안 사례를 참조하십시오.
- Security-Enhanced Linux 설명서.