Firepower System 릴리스 노트

버전 6.0
최초 발행: 2015년 11월 11일 목요일
최종 업데이트: 2016년 6월 13일

이 릴리스 노트는 Firepower System의 버전 6.0에 적용됩니다. 업데이트 프로세스를 잘 알고 있더라도 릴리스 노트를 꼼꼼하게 읽고 이해하십시오. 릴리스 노트에는 지원되는 플랫폼, 새로운 기능과 변경된 기능, 관리 플랫폼과 관리되는 디바이스 간의 호환성, 알려진 문제와 해결된 문제가 설명되어 있습니다. 릴리스 노트에는 또한 전제 조건, 경고 및 특정 설치 지침에 관한 자세한 정보가 포함되어 있습니다.

정보 Firepower System용 설명서 전문에 액세스하려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html에서 문서 로드맵을 확인하십시오.

주의: 버전 6.0으로 업데이트하기 전에 반드시 FireSIGHT System Version 6.0.0 설치-전 패키지를 설치해야 합니다. 자세한 내용은 *FireSIGHT System 릴리스 노트 버전 6.0 설치-전 패키지*를 참조하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

지원되는 플랫폼 및 호환성

지원되는 플랫폼, 최소 시작 버전 및 운영 체제는 버전별로 다릅니다. 자세한 내용은 다음 링크를 참고하십시오.

지원되는 플랫폼

버전 6.0은 다음 표에 명시된 플랫폼에서 실행할 수 있습니다. Firepower System의 최소 버전 요구 사항은 버전 6.0 업데이트를 위한 FirePower 버전 요구 사항, 13페이지를 참조하십시오.

참고: 일부 Firepower Management Center 모델(이전 명칭: FireSIGHT Management Center 또는 Defense Center)의 경우, Firepower 버전 6.0에 이전 버전보다 더 많은 메모리가 필요합니다. 구체적으로, MC750에는 2개의 4GB DIMM(Dual In-line Memory Module)이 필요합니다. 마찬가지로 6GB 메모리가 장착된 MC1500에도 추가 메모리가 필요합니다.

표 2-1 버전 6.0의 플랫폼 지원

버전 6.0에서 지원되는 플랫폼	버전 6.0의 기능	버전 6.0 실행을 위한 기타 요구 사항
Firepower Management Center(MC750, MC1500, MC3500, MC2000, MC4000)	방지	■ MC750에는 2개의 4GB DIMM(Dual In-line Memory Module) 필요 ■ MC1500에는 최소 8GB 메모리 필요
64-비트 Firepower Management Center Virtual	방지	호스팅 위치: ■ VMware vSphere Hypervisor/VMware ESXi 5.1 ■ VMware vSphere Hypervisor/VMware ESXi 5.5 ■ VMware vCloud Director 5.1
Firepower 7000 Series 및 8000 Series(7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390)	관리되는 디바이스	해당 없음
Cisco ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, AS A5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)	관리되는 디바이스	ASA 버전 9.4(2) 또는 9.5(2) 실행
NGIPSv(가상 관리 디바이스)	관리되는 디바이스	호스팅 위치: ■ VMware vSphere Hypervisor/VMware ESXi 5.1 ■ VMware vSphere Hypervisor/VMware ESXi 5.5 ■ VMware vCloud Director 5.1

관리 플랫폼과 관리되는 디바이스 간의 호환성

관리 기능은 버전별로 다릅니다. 다음 표에는 사용 가능한 관리 플랫폼과 각 플랫폼에서 관리하는 디바이스가 상세히 명시되어 있습니다.

표 2-2 관리 플랫폼-관리 플랫폼별 호환성

지원되는 관리 플랫폼	이 관리 플랫폼을 사용하여 관리할 수 있는 디바이스
Firepower Management Centers(MC750, MC1500, MC3500, MC2000, MC4000)	버전 5.4.0.6 이상을 실행 중인 아래의 모든 디바이스: ■ Firepower 7000 Series 및 8000 Series (7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390) ■ NGIPSv(가상 관리 디바이스) ■ Cisco ASA with Firepower Services(ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60) 버전 5.4.1.5를 실행 중인 아래의 모든 디바이스: ■ Cisco ASA with Firepower Services(ASA 5506X- ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X) 버전 6.0을 실행 중인 아래의 모든 디바이스: ■ Firepower 7000 Series 및 8000 Series(7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390) ■ NGIPSv(가상 관리 디바이스) ■ Cisco ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)

표 2-2 관리 플랫폼-관리 플랫폼별 호환성

지원되는 관리 플랫폼	이 관리 플랫폼을 사용하여 관리할 수 있는 디바이스
ASDM 버전 7.5(1.112)	버전 6.0을 실행 중인 아래의 모든 디바이스: ■ 시스코 ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)
64-비트 Firepower Management Centers Virtual	버전 5.4.0.6 이상을 실행 중인 아래의 모든 디바이스: ■ Firepower 7000 Series 및 8000 Series (7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390) ■ NGIPSv(가상 관리 디바이스) ■ Cisco ASA with Firepower Services(ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60) 버전 5.4.1.5를 실행 중인 아래의 모든 디바이스: ■ Cisco ASA with Firepower Services(ASA 5506X- ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X) 버전 6.0을 실행 중인 아래의 모든 디바이스: ■ Firepower 7000 Series 및 8000 Series(7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390) ■ NGIPSv(가상 관리 디바이스) ■ 시스코 ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)

표 2-3 관리 플랫폼-관리되는 디바이스의 관리되는 디바이스별 호환성

지원 대상인 관리되는 디바이스	이 디바이스 관리에 사용 가능한 플랫폼
Firepower 7000 Series 및 8000 Series(7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390)	버전 6.0을 실행 중인 아래의 모든 디바이스: ■ Firepower Management Centers(MC750, MC1500, MC3500, MC2000, MC4000) ■ 64-비트 Firepower Management Centers Virtual
Cisco ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)	버전 6.0을 실행 중인 아래의 모든 디바이스: ■ Firepower Management Centers(MC750, MC1500, MC3500, MC2000, MC4000) ■ 64-비트 Firepower Management Centers Virtual ■ ASDM(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)
NGIPSv(가상 관리 디바이스)	버전 6.0을 실행 중인 아래의 모든 디바이스: ■ Firepower Management Centers(MC750, MC1500, MC3500, MC2000, MC4000) ■ 64-비트 가상 Firepower Management Centers

새로운 기능

릴리스 노트의 본 섹션에서는 Firepower System 버전 6.0에 포함된 새로운 기능과 업데이트된 기능을 설명합니다.

■ 새로운 기능, 5페이지
■ 기능 변경 사항, 8페이지
■ 업데이트된 용어, 8페이지
■ 업데이트된 문서, 8페이지

새로운 기능

다음은 버전 6.0에 도입된 기능입니다.

위협 차단 강화

URL 및 DNS-기반 보안 인텔리전스

URL 및 DNS(Domain Name System) 서버를 기반으로 하는 새로운 보안 인텔리전스 피드가 제공되어 기존의 IP-기반 보안 인텔리전스 기능이 개선되었습니다. 현재 IP 기반 인텔리전스는 알려진 악성코드, 피싱(phishing), 명령 및 제어, 그리고 봇 사이트에 대한 액세스를 제어하는 데 사용되고 있습니다. IP 기반 인텔리전스를 우회하도록 설계된 새로운 공격 방식(예: Fast Flux)은 악의적인 서버의 실제 IP 주소를 은폐하기 위해 DNS 부하 분산 기능을 악용합니다. 공격에 사용되는 IP 주소는 수시로 바뀌는 반면, 도메인 이름은 변경되는 경우가 드뭅니다. UR-기반 인텔리전스로 IP-기반 인텔리전스를 보완하여 이러한 공격 유형에 대처할 수 있으며, DNS-기반 인텔리전스는 이러한 유형의 공격과 연관된 알려진 DNS 서버를 식별하는 데 도움이 됩니다. 새로운 인텔리전스 피드를 사용하여 액세스 컨트롤 정책을 생성할 수 있으며, 새로운 대시보드에서는 가시성과 분석 역량을 제공합니다. 또한 URL-기반 및 DNS-기반 보안 인텔리전스 이벤트는 둘 다 IoC(Indications of Compromise) 상관관계 기능으로 입력됩니다. 이 두 가지 새로운 피드는 Cisco Talos Security Intelligence and Research Group에서 제공하는 정기적인 업데이트를 통해 제공되며, IP-기반 보안 인텔리전스 기능과 마찬가지로 기본 제품에 포함되어 있으므로 별도의 라이센스가 필요하지 않습니다.

DNS 인스펙션 및 싱크홀

자신들의 활동을 은폐하기 위해 SSL 프로토콜을 사용하는 공격자들은 같은 의도로 DNS 프로토콜을 사용합니다. 이와 같은 이유와 더불어 Fast Flux-유형의 공격에 대처하기 위해 Firepower 시스템에서는 DNS 트래픽 요청을 가로채고 정책 설정에 따라 적절한 조치를 취합니다. DNS 정책을 사용하면 알려진 명령 및 제어/스팸/피싱 및 차단해야 하는 사이트로 요청을 보내거나 요청에 대해 `Domain Not Found` 메시지를 반환하거나 트래픽을 사전-구성된 싱크홀로 보낼 수 있습니다. 마지막 옵션은 트래픽을 Firepower에서 관리되는 디바이스로 직접 라우팅한 다음 IoC 경고를 유발할 수 있는 엔드포인트에 관한 정보를 제공합니다.

향상된 네트워크 가시성 및 제어

ASDM을 통해 관리되는 Cisco ASA with FirePOWER Services용 SSL 해독

시스코의 차세대 방화벽(NGFW)인 Cisco ASA with FirePOWER Services가 이제 공격, 애플리케이션 및 악성코드 탐지를 수행하기 전에 SSL 통신을 로컬에서 관리하고 트래픽을 해독할 수 있습니다. 이는 시스코의 Firepower 차세대 IPS(NGIPS) 어플라이언스 버전 5.4에 도입된 것과 동일한 기능입니다. SSL 해독은 수동 모드나 인라인 모드로 구축할 수 있으며, HTTPS 및 StartTLS-기반 애플리케이션(예: SMTPS, POP3S, FTPS, IMAPS, TelnetS)을 지원합니다. 개인 정보 보호를 강화하기 위해 URL 카테고리에 따라 해독을 제한하는 등 암호화된 트래픽의 기록 및 처리를 세밀하게 제어하도록 해독 정책을 구성할 수 있습니다. 또한 자체-서명된 암호화 트래픽을 차단하거나 SSL 버전, 특정 Cipher Suites 및/또는 승인되지 않은 모바일 디바이스를 차단할 수 있습니다.

OpenAppID-정의 애플리케이션 지원

시스코에서 제공하는 OpenAppID는 오픈 소스를 기반으로 하는 애플리케이션-중심의 탐지 언어로, 사용자가 NGFW 벤더의 릴리스 주기나 로드맵에 종속되지 않고 새로운 애플리케이션 탐지 서명을 생성, 공유 및 구축하여 사용자 지정, 로컬 및 클라우드 애플리케이션을 만들 수 있도록 지원합니다. 버전 6.0에서는 3,000여 개의 애플리케이션을 식별하고 액세스를 제어하는 Firepower 애플리케이션 탐지 엔진이 OpenAppID-정의 애플리케이션을 인식할 수 있도록 개선되었습니다. Snort가 침입 탐지 분야를 오픈 소스로 전환하기 위한 노력의 일환이었던 것처럼, OpenAppID는 애플리케이션 탐지 분야를 오픈 소스로 전환하려는 노력입니다. 시스코는 이 오픈 소스 이니셔티브를 이끌고 고객에게 향상된 유연성을 제공하기 위해 OpenAppId 정의 애플리케이션을 지원하고 있습니다.

Captive Portal 및 Active Authentication

브라우저 창에서 사용자에게 자격 증명을 입력하라는 메시지가 표시도록 Captive Portal 및 Active Authentication 기능을 구성하면, 사용자를 IP 주소 및 관련 네트워크 이벤트로 매핑할 때 더 나은 가시성을 제공할 수 있습니다. 이러한 매핑을 통해 사용자 또는 사용자 그룹을 기반으로 정책을 설정할 수 있습니다. 이 기능은 기존의 SUA(Sourcefire User Agent)와 Active Directory의 통합을 보완하여 Windows-이외의 환경, BYOD 사용자 및 게스트를 지원합니다.

참고: ASA 버전 9.5(2) 이상을 실행 중인 경우에만 Cisco ASA with FirePOWER Services에서 Captive Portal 및 Active Authentication 기능을 사용할 수 있습니다.

Cisco ISE(Identity Services Engine)와 통합

시스코 ISE와 통합되어 시스템에서 분석 및 정책 제어 시 사용하는 사용자 ID 데이터가 강화되었습니다. Firepower Management Center에서는 시스코의 PxGrid(Platform Exchange Grid)를 구독하여 추가적인 사용자 데이터, 디바이스 유형 데이터, 디바이스 위치 데이터 및 SGT(Security Group Tag, 네트워크 액세스 제어 기능을 제공하기 위해 ISE에서 사용하는 방법)를 다운로드합니다. 이러한 데이터는 네트워크상의 사용자에 대한 추가적인 가시성을 제공할 뿐만 아니라 SGT, 디바이스 유형 또는 ISE에서 제공되는 그 밖의 정보를 기반으로 정책을 생성할 수 있도록 함으로써 향상된 제어를 제공하는 유용한 인텔리전스이기도 합니다.

참고: 버전 6.0에서는 ISE를 사용하여 감염된 엔드포인트를 자동으로 격리할 수 없습니다. 이 기능은 이후 릴리스에 포함될 예정입니다.

Advanced Persistent Threat을 방어하는 개선된 위협 방어

로컬 악성코드 검사

이 기능을 사용하면 널리 사용되는/일반적인 악성코드를 Firepower 어플라이언스에서 직접 식별할 수 있으며, 클라우드나 온-프레미스에서 동적 분석을 위해 파일을 전송(샌드박싱)할 필요가 줄어듭니다(AMP Threat Grid와의 통합 참조). SHA-256 조회 결과 `Unknown`이 반환되는 파일은 신뢰도가-높은 ClamAV 서명을 사용하여 Firepower 어플라이언스에서 로컬로 분석되어 악성코드와 관련된 일반적인 특성을 식별함으로써 동적 분석의 필요를 줄여줍니다.

파일 속성 분석

특정 파일 유형은 악성코드를 숨기는 데 사용될 수 있는 중첩된 콘텐츠를 지원합니다. 이 기능으로 파일을 로컬에서 분석하여 악성코드가 은폐되어 있는지 확인합니다. 예를 들어, PDF 파일에는 다양한 유형의 파일이 중첩되어 있을 수 있습니다. 그런 다음 해당 파일 내부에 중첩된 데이터가 존재하는지, 중첩된 파일의 유형이 무엇인지, 중첩된 파일에 악성코드가 포함되어 있을 가능성은 어느 정도인지 식별하는 파일 구성 보고서가 생성됩니다. 사용자는 이 정보를 보고 해당 파일을 동적 분석으로 처리할지 결정할 수 있습니다.

AMP 위협 그리드와의 통합

2014년 6월에 ThreatGrid가 시스코에 인수되면서, 고객이 Advanced Persistent Threat에 더 잘 대응하도록 지원할 수 있게 되었습니다. 이제 Firepower v6.0에 이 기술이 완벽하게 통합되어, AMP Threat Grid에서 **Firepower용 AMP** 옵션을 사용하면 클라우드에서 샌드박싱 기능을 사용할 수 있습니다. 동적 분석을 위해 클라우드로 전송된 파일은 분석된 수억 개의 다른 악성코드 아티팩트와의 비교를 통해 안전하게 분석되고 상관관계가 도출되어 악성코드 공격, 캠페인 및 분산에 대한 종합적인 관점을 제공합니다. 상세 보고서를 통해 주요 행동 지표를 식별하고 신속한 우선순위 선정을 위해 위협 점수를 산정하여 지능형 공격으로부터 복구합니다.

또한 자동 동적 분석이 지원되는 파일 유형을 대폭 추가했습니다. 이제 실행 파일뿐만 아니라 PDF 및 Office 문서도 지원됩니다.

관리 기능 강화

여러 도메인 관리

이제 Firepower Management Center로 여러 관리 도메인을 생성할 수 있습니다. 따라서 개별적인 고객 환경을 관리해야 하는 통신 사업자와 개별적으로 관리되어야 하는 기업이나 사업부를 인수(중복되는 IP 주소 발생)한 엔터프라이즈에서 여러 도메인을 관리할 수 있게 되었습니다. 여러 도메인(최대 50개)을 생성하면 관리 환경을 분리할 수 있으며, 각 도메인은 세밀한 RBAC(Role-Based Access Control)를 사용하여 관리됩니다. 각 도메인에서는 개별적인 이벤트 데이터, 보고 및 네트워크 맵을 제공합니다.

정책 계층 구조 및 상속

Version 6.0에서는 정책을 계층 구조로 생성할 수 있는 기능을 제공하므로 여러 도메인의 관리를 지원하고 정책 관리를 효율적으로 수행할 수 있습니다. 먼저 모든 관리 환경에 적용되는 글로벌 정책(액세스 컨트롤 등)을 수립합니다. 그런 다음 여러 환경, 여러 회사, 여러 사업부 또는 여러 조직을 나타낼 수 있도록 글로벌 정책 레벨 아래에 정책 계층 구조를 구성합니다. 각 정책 환경은 상위 계층의 정책을 상속하기 때문에 보다 일관적이고 효율적인 정책 관리가 가능해집니다.

ASDM 관리 가용성 강화

시스코의 ASDM(Adaptive Security Device Manager)은 Cisco ASA with FirePOWER Services용 로컬 관리 기능입니다. ASDM은 시스코 ASA 5506-X, ASA 5508-X 및 ASA 5516-X 어플라이언스의 일부로 도입되었습니다. Firepower v6.0부터 나머지 Cisco ASA with FirePOWER Services 어플라이언스(ASA 5512-X / ASA 5515-X / ASA 5525-X / ASA 5545-X / ASA 5555-X / ASA 5585-X)에서도 ASDM을 사용할 수 있습니다.

기능 변경 사항

- NAT 정책 페이지, 플랫폼 설정 페이지 및 SSL 정책 페이지에서 정책을 비교할 수 없습니다.
- 버전 6.0에서는 프라이빗 AMP 클라우드의 Firepower용 AMP 서명 조회 기능이 지원되지 않습니다. 버전 6.0에서는 시스템이 퍼블릭 AMP 클라우드로 SHA-256 서명을 자동으로 제출합니다. 프라이빗 AMP 클라우드를 사용 중이며 엔드포인트로부터 이벤트를 수신하는 경우, 컨피그레이션을 변경하지 않아도 계속해서 버전 6.0 Firepower Management Center로 이벤트를 수신할 수 있습니다.
- 이제 HTTP Referrer, User Agent, Referenced Host 필드에 연결 이벤트용 시스템 로그 메시지가 포함됩니다.
- 버전 6.0에서는 Discovery Event Health Monitoring을 지원하지 않습니다.)
- 이제 FirePOWER Services를 실행 중인 ASA 모듈에서 AAB(Automatic Application Bypass) 설정을 편집할 수 있습니다.

업데이트된 용어

버전 6.0에서 사용되는 용어는 이전 릴리스에서 사용된 용어와 다를 수 있습니다. 자세한 내용은 *Firepower 호환 가이드*를 참조하십시오.

업데이트된 문서

Firepower System용 설명서 전문에 액세스하려면 http://www.cisco.com/c/en/us/td/docs/security/firesight/roadmap/firesight-roadmap.html 에서 문서 로드맵을 확인하십시오. 버전 6.0에서는 새로운 기능과 변경된 기능을 반영하고 보고된 문서 문제를 해결하기 위해 다음과 같은 문서가 업데이트되었습니다.

- *Firepower Management Center 온라인 도움말*
- *ASA FirePOWER 모듈 온라인 도움말*
- *Firepower Management Center 컨피그레이션 가이드*
- *Firepower Management Center 설치 가이드*
- *Firepower System Virtual 설치 가이드*
- *Firepower System eStreamer 통합 가이드*
- *Firepower System Remediation API 설명서*
- *Firepower System Database Access 설명서*
- *Firepower System Host Input API 설명서*
- Firepower NGIPSv for VMware 빠른 시작 가이드
- Firepower NGIPSv 및 Firepower Management Center for VMware 빠른 시작 가이드
- Cisco ASA FirePOWER Services Local Management 컨피그레이션 가이드
- Firepower 7000 및 8000 Series 설치 가이드

버전 6.0에 대한 업데이트된 문서에는 다음과 같은 오류가 포함되어 있습니다.

- *Firepower Management Center 컨피그레이션 가이드*에는 다중 도메인 구축 환경에서 DNS 정책을 생성할 때 DNS 규칙용 상속자 화이트리스트와 DNS 규칙용 상속자 블랙리스트가 기본으로 사용 중지된다는 사실이 반영되어 있지 않습니다. 해당 화이트리스트와 블랙리스트는 각 규칙을 편집하여 사용 설정할 수 있습니다. (CSCuw62140)
- 온라인 도움말에서는 정책 적용이 사용 설정되고 Snort 재시작이 필요한 컨피그레이션이 없을 때 트래픽 검사를 사용하여 컨피그레이션 변경 사항을 구축하면 정책 구축 중에 현재 구축된 액세스 컨트롤 정책이 아닌 기본값인 침입 정책이 트래픽을 검사하는 것으로 잘못 기재되어 있습니다.

참고: 온라인 도움말 콘텐츠는 *Firepower Management Center컨피그레이션 가이드* 콘텐츠와 다를 수 있습니다. 온라인 도움말보다는 *Firepower Management Center 컨피그레이션 가이드*의 콘텐츠가 더 정기적으로 업데이트됩니다.

시작하기 전에: 중요 업데이트 및 호환성 정보

버전 6.0 업데이트 프로세스를 시작하기 전에 업데이트 프로세스 중의 시스템 행동과 호환성 문제 또는 필수 업데이트 사전- 또는 사후-업데이트 컨피그레이션 변경 사항을 숙지해야 합니다.

주의: 버전 6.0으로 업데이트 하기 전에 반드시 FireSIGHT 시스템 버전 6.0.0 설치-전 패키지를 설치해야 합니다. 자세한 내용은 *FireSIGHT 시스템 릴리스 노트 버전 6.0 설치-전 패키지* 를 참조하십시오.

주의: 시스코에서는 유지 보수 기간 중 또는 중단으로 인해 구축에 미치는 영향이 최소화되는 때에 업데이트를 수행하는 것을 권장합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 컨피그레이션 및 이벤트 백업 지침, 9페이지
- 업그레이드 전에 Firepower Management Center 고가용성 쌍 해제, 10페이지
- MC750, MC1500, Management Centers Virtual의 Firepower Management Center 메모리 업데이트, 10페이지
- Management Center HTTPS 인증서를 버전 6.0으로 업데이트, 10페이지
- 업데이트 도중 트래픽 흐름 및 검사, 11페이지
- 업데이트 중의 감사 로깅, 12페이지
- 버전 6.0 업데이트를 위한 시간 및 디스크 공간 요구 사항, 12페이지
- Management Center HTTPS 인증서를 버전 6.0으로 업데이트, 10페이지
- 버전 6.0의 웹 브라우저 및 화면 해상도 호환성, 13페이지
- 버전 6.0에 통합된 제품 호환성, 14페이지

컨피그레이션 및 이벤트 백업 지침

시스코에서는 업데이트를 시작하기 전에 어플라이언스에 있는 백업 파일을 삭제하거나 이동한 다음 현재 이벤트 및 컨피그레이션 데이터를 외부 위치로 백업할 것을 권장합니다.

Firepower Management Center를 사용하여 자체 및 여기에서 관리하는 디바이스의 이벤트와 컨피그레이션 데이터를 백업하십시오. 백업 및 복원 기능에 대한 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*를 참조하십시오.

버전 6.0에서는 프라이빗 AMP 클라우드의 Firepower용 AMP 서명 조회 기능이 지원되지 않습니다. 버전 6.0에서는 시스템이 퍼블릭 AMP 클라우드로 SHA-256 서명을 자동으로 제출합니다. 프라이빗 AMP 클라우드를 사용 중이며 엔드포인트로부터 이벤트를 수신하는 경우, 컨피그레이션을 변경하지 않아도 계속해서 버전 6.0 Firepower Management Center로 이벤트를 수신할 수 있습니다.

참고: Firepower Management Center는 이전 업데이트에서 로컬에 저장된 백업을 제거합니다. 보관된 백업을 보존하려면 외부 장치에 백업을 저장하십시오.

업그레이드 전에 Firepower Management Center 고가용성 쌍 해제

버전 6.0에서는 고가용성 쌍에 포함된 Firepower Management Centers를 지원하지 않습니다. 고가용성 환경에서 Firepower Management Centers를 업데이트하려면 먼저 쌍을 해제한 다음 각 Firepower Management Center를 개별적으로 업데이트해야 합니다. 버전 6.0으로 업데이트하려면 고가용성 쌍을 해제해야 합니다.

MC750, MC1500, Management Centers Virtual의 Firepower Management Center 메모리 업데이트

일부 Firepower Management Center 모델(이전 명칭: FireSIGHT Management Center 또는 Defense Center)의 경우 Firepower 버전 6.0에 이전 버전보다 더 많은 메모리가 필요합니다. 구체적으로, MC750에는 2개의 4GB DIMM(Dual In-line Memory Module)이 필요합니다. 마찬가지로 6GB 메모리가 장착된 MC1500에도 추가 메모리가 필요합니다.

시스코 제품 요구 사항에 따라 메모리가 증가했기 때문에, 시스코에서는 해당 모델을 보유한 고객에게 메모리 업그레이드 키트를 제공하고 있습니다. 해당 MC750 또는 MC1500 Firepower Management Center 모델에서 버전 6.0을 실행할 권한이 있는 고객은 메모리 업그레이드 키트를 무상으로 주문할 수 있습니다.

메모리 키트 주문에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html을 참조하십시오. 키트를 받은 다음 메모리를 교체하는 방법에 대한 지침은 *Firepower Management Center 설치 가이드*의 "Firepower Management Centers용 메모리 업그레이드 지침"을 참조하십시오.

Management Centers Virtual을 버전 6.0으로 업데이트하려면 최소 8GB의 메모리가 필요합니다.

Management Center HTTPS 인증서를 버전 6.0으로 업데이트

Firepower Management Center에서 `RSASSA-PSS` 서명 알고리즘을 가진 인증서를 사용하는 것은 현재 버전 6.0에서 지원하지 않습니다. 이러한 인증서를 사용하는 Firepower Management Center를 버전 6.0으로 업데이트하거나 버전 6.0에 이러한 인증서를 추가하면 Management Center 웹 인터페이스에 로그인할 수 없고, 시스템에서 `Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator` 오류가 발생합니다.

업데이트를 수행하기 전에 `sha1WithRSAEncryption` 또는 `sha256WithRSAEncryption` 알고리즘의 HTTPS 인증서를 생성하여 설치한 다음 Firepower Management Center를 재시작하거나 기본 Firepower Management Center 인증서를 사용한 다음 어플라이언스를 재시작하십시오.

이와 마찬가지로, Firepower Management Center에서 사용 중인 인증서가 2048비트보다 큰 공개 서버 키로 생성되었다면 버전 6.0으로 업데이트한 다음에 Management Center 웹 인터페이스에 로그인할 수 없습니다.

2048비트보다 큰 공개 서버 키로 Management Center 웹 인터페이스에 로그인할 수 없는 경우, CSR(Server Certificate Request)을 생성하여 인증서를 생성하고 생성된 인증서를 Firepower Management Center에 적용함으로써 크기가 큰 공개 키로 생성된 인증서를 대체하십시오. 새 인증서를 설치한 후 어플라이언스를 재시작합니다.

참고: 버전 5.4.x 어플라이언스에서 인증서를 올바르게 생성하는 방법에 대한 자세한 정보는 *FireSIGHT System 사용 설명서* 버전 5.4.1의 사용자 지정 HTTPS 인증서 사용을 참조하십시오.

버전 6.0으로 업데이트하거나 인증서를 업로드한 뒤에 웹 인터페이스에 액세스할 수 없는 경우에는 Support(지원팀)로 문의하십시오.

업데이트 도중 트래픽 흐름 및 검사

업데이트 프로세스중에는 관리되는 디바이스가 재부팅됩니다. Snort 프로세스도 재시작될 수 있습니다. 디바이스가 어떻게 구성되고 구축되었는지에 따라 다음과 같은 기능이 영향을 받을 수 있습니다.

- 애플리케이션 인식 및 제어, URL 필터링, 보안 인텔리전스, 침입 탐지 및 방지, 연결 로깅을 비롯한 트래픽 검사
- 스위칭, 라우팅, NAT, VPN 및 관련 기능을 비롯한 트래픽 흐름
- 링크 상태

8000 Series 클러스터나 스택 쌍을 업데이트하는 경우 시스템에서 트래픽 중단을 방지하기 위해 한 번에 하나의 디바이스에 대한 업데이트를 수행합니다. 클러스터링된 Cisco ASA with FirePOWER Services 디바이스를 업데이트하는 경우에는 한 번에 하나의 디바이스를 업데이트하고, 업데이트가 완료된 다음에 다른 디바이스를 업데이트하십시오.

다음 표에는 Snort 재시작이 트래픽 검사에 어떤 식으로 영향을 주는지 설명되어 있습니다. 제품 업데이트 시 트래픽이 이와 유사하게 영향을 받을 것이라고 생각할 수 있습니다.

Link State

바이패스가 사용 설정된 7000 Series 및 8000 Series 인라인 구축에서는 업데이트 시에 다음과 같은 두 시점에 네트워크 트래픽이 중단됩니다.

- 업데이트 프로세스가 시작될 때 링크가 끊겼다 연결되었다 하고 네트워크 카드가 하드웨어 바이패스로 전환되며 트래픽이 잠시 중단됩니다. 하드웨어 바이패스 중에는 트래픽 검사가 수행되지 않습니다.
- 업데이트가 끝나는 시점에 링크가 끊겼다 연결되었다 하고 네트워크 카드가 바이패스에서 기존 상태로 전환되며 트래픽이 다시 한 번 잠시 중단됩니다. 엔드포인트가 다시 연결되고 센서 인터페이스와의 링크가 복구되면 트래픽 검사가 다시 수행됩니다.

NGIPSv 디바이스, Cisco ASA with FirePOWER Services, Firepower 8000 Series 디바이스의 논-바이패스 NetMods, 71xx 제품군 디바이스의 SFP 트랜시버, Firepower Threat Defense를 실행 중인 ASA Firepower 모듈에서는 **바이패스** 옵션을 구성할 수 **없습니다**.

표 2-4 네트워크 트래픽 중단

관리되는 디바이스 모델	다음과 같이 구성	재시작 시 트래픽 상태
7000 Series, 8000 Series, NGIPSv	**Failsafe**가 사용 설정 또는 사용 중지된 인라인 또는 인라인 탭 모드	검사 없이 통과됨(**Failsafe**가 사용 중지되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음)
	수동	중단되지 않음, 검사되지 않음
7000 Series 및 8000 Series	라우팅, 스위칭 또는 투명	삭제됨
Cisco ASA with FirePOWER Services	라우팅 또는 fail-open 상태로 투명(**트래픽 허용**)	검사 없이 통과됨
	라우팅 또는 fail-close 상태로 투명(**트래픽 차단**)	삭제됨

스위칭 및 라우팅

Firepower 7000 Series 및 8000 Series의 관리되는 디바이스는 업데이트 중에 스위칭, 라우팅, NAT, VPN 또는 관련 기능을 수행하지 **않습니다**. 스위칭 및 라우팅만 수행하도록 디바이스를 구성한 경우, 업데이트가 진행되는 내내 네트워크 트래픽이 차단됩니다.

업데이트 중의 감사 로깅

웹 인터페이스를 사용하는 어플라이언스를 업데이트하는 경우, 시스템에서 업데이트-사전 작업을 마치고 간소화된 업데이트 인터페이스 페이지가 나타나면 업데이트 프로세스가 완료되고 어플라이언스가 재부팅되기 전까지 어플라이언스에 대한 로그인 시도가 감사 로그에 반영되지 않습니다.

버전 6.0 업데이트를 위한 시간 및 디스크 공간 요구 사항

아래 표에서는 버전 6.0 업데이트를 위한 시간 및 디스크 공간 지침이 제공됩니다. 관리되는 디바이스를 Firepower Management Center를 사용하여 업데이트하는 경우에는 Firepower Management Center의 `/Volume` 파티션에 추가 디스크 공간이 필요합니다.

주의: 업데이트 프로세스 도중에는 절대로 업데이트를 재시작하거나 어플라이언스를 재부팅하지 마십시오. 시스코에서는 참고를 위해 예상 시간을 제공하고 있으나, 실제 업데이트에 걸리는 시간은 어플라이언스 모델, 구축 및 컨피그레이션에 따라 달라질 수 있습니다. 업데이트의 사전-확인 시점과 재부팅된 이후 시점에 시스템이 비활성화된 것으로 보일 수 있으나, 이는 정상적인 동작입니다.

업데이트 도중 재부팅이 수행될 때 데이터베이스 확인이 수행됩니다. 데이터베이스 확인 도중에 오류가 발견되면 업데이트에 시간이 더 소요될 수 있습니다. 데이터베이스 확인 및 복구 중에는 데이터베이스와 상호 작용하는 시스템 데몬이 실행되지 않습니다.

참고: 어플라이언스에 설치된 버전이 릴리스 버전(버전 6.0)에 가까울수록 업데이트에 걸리는 시간이 줄어듭니다.

업데이트에 문제가 있는 경우 Support(지원팀)로 문의하십시오.

표 2-5 시간 및 디스크 공간 요구 사항

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager /Volume에 필요한 공간	시간
Firepower Management Centers(MC750, MC1500, MC3500, MC2000, MC4000)	16 MB	8022 MB	1.5 GB	58분
64-비트 Firepower Management Centers Virtual	16 MB	8022 MB	1.5 GB	하드웨어에 따라 다름
7000 Series 및 8000 Series 디바이스(7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390)	16 MB	6496 MB	1.2 GB	94분
Cisco ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)	32 MB	7644 MB	1.2 GB	41분
NGIPSv(가상 관리 디바이스)	17 MB	6046 MB	1.2 GB	하드웨어에 따라 다름

버전 6.0 업데이트를 위한 FirePower 버전 요구 사항

Firepower System 버전 6.0으로 업데이트하려면 다음 표에서 볼 어플라이언스가 수 있는 최소 버전을 실행 중이어야 합니다. 운영 체제 최소 요구 사항 및 관리 플랫폼-관리되는 디바이스 사이의 호환성에 관한 정보는 지원되는 플랫폼 및 호환성, 1페이지를 참조하십시오.

참고: Firepower Management Center를 사용하여 해당 관리되는 디바이스를 버전 6.0으로 업데이트하려면 버전 6.0 이상을 실행 중이어야 합니다.

표 6 버전 6.0의 플랫폼 지원

플랫폼	버전 6.0 업데이트를 위한 최소 버전 요구 사항
Firepower Management Centers(MC750, MC1500, MC3500, MC2000, MC4000)	버전 5.4.1
64-비트 Firepower Management Centers Virtual	버전 5.4.1
Firepower 7000 Series 및 8000 Series(7010, 7020, 7030, 7050, 7110, 7115,7120, 7125,8120, 8130, 8140, 8250,8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8380, AMP8390)	버전 5.4.0.6
Cisco ASA with FirePOWER Services(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X)	버전 5.4.1
Cisco ASA with FirePOWER Services(ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60)	버전 5.4.0.6
NGIPSv(가상 관리 디바이스)	버전 5.4.0.6

버전 6.0의 웹 브라우저 및 화면 해상도 호환성

웹 인터페이스 경험을 최적화려면 다음 사항을 확인하십시오.

웹 브라우저 호환성

Firepower System의 웹 인터페이스 버전 6.0은 다음 표에 나열된 브라우저에서 테스트되었습니다.

참고: Microsoft Internet Explorer 11 브라우저를 사용하는 경우에는 Internet Explorer 설정의 **도구 \> 인터넷 옵션 \> 보안 \> 사용자 지정 수준**에서 **파일을 서버에 업로드할 때 로컬 디렉터리 경로 포함** 옵션을 사용 안 함으로 설정해야 합니다.

표 7 지원되는 웹 브라우저

브라우저	필수 활성화 옵션 및 설정
Chrome 46	JavaScript, 쿠키
Firefox 41	JavaScript, 쿠키, SSL(Secure Sockets Layer) v3
Microsoft Internet Explorer 10 및 11	JavaScript, 쿠키, SSL(Secure Sockets Layer) v3, 128비트 암호화, **액티브 스크립팅** 보안 설정, 호환성 보기, set **저장된 페이지의 새 버전 확인**을 **자동으로 설정**

화면 해상도 호환성

시스코에서는 가로 크기가 최소 1280픽셀인 화면 해상도를 선택할 것을 권장합니다. 사용자 인터페이스는 낮은 해상도에서도 호환되지만, 높은 해상도에서 디스플레이가 최적화됩니다.

버전 6.0에 통합된 제품 호환성

아래와 같은 통합된 제품에 필요한 버전은 Firepower System 버전에 따라 달라집니다.

- Cisco ISE(Identity Services Engine)
- Cisco AMP Threat Grid
- Cisco Firepower System User Agent

자세한 내용은 *Firepower System 호환 가이드*를 참조하십시오.

업데이트 설치

업데이트를 시작하기 전에 본 릴리스 노트를(특히 지원되는 플랫폼 및 호환성, 1페이지 및 시작하기 전에: 중요 업데이트 및 호환성 정보, 9페이지) 철저하게 읽고 이해해야 합니다.

Firepower System의 최소 버전 요구 사항은 버전 6.0 업데이트를 위한 FirePower 버전 요구 사항, 13페이지를 참조하십시오. 어플라이언스를 업데이트하려면 아래의 지침과 절차를 확인하십시오.

- Firepower Management Centers 업데이트, 15페이지
- 관리되는 디바이스 및 ASA FirePOWER 모듈 업데이트, 17페이지

주의: 업데이트 도중에는 로그인 프롬프트가 표시될 때까지 어플라이언스를 절대로 재부팅하거나 종료하지 마십시오. 업데이트의 사전-확인 시점에 시스템이 비활성화된 것으로 보일 수 있습니다. 이것은 정상적인 동작이므로 어플라이언스를 재부팅하거나 종료할 필요가 없습니다.

참고: 일부 Firepower Management Center 모델(이전 명칭: FireSIGHT Management Center 또는 Defense Center)의 경우, Firepower 버전 6.0에 이전 버전보다 더 많은 메모리가 필요합니다. 구체적으로, MC750에는 2개의 4GB DIMM(Dual In-line Memory Module)이 필요합니다. 마찬가지로 6GB 메모리가 장착된 MC1500에도 추가 메모리가 필요합니다. 자세한 내용은 MC750, MC1500, Management Centers Virtual의 Firepower Management Center 메모리 업데이트, 10페이지 및 *Firepower Management Center 설치 가이드*를 참조하십시오.

주의: 버전 5.4.0.5 이하를 실행 중인 관리되는 디바이스를 보유한 시스템을 버전 6.0으로 업데이트하면 트래픽 중단 및 시스템 문제가 발생할 수 있습니다. 버전 6.0으로 업데이트하기 전에 반드시 관리되는 디바이스를 버전 5.4.0.6 이상으로 업데이트하십시오.

업데이트 수행 시기

업데이트 프로세스는 트래픽 검사, 트래픽 흐름 및 링크 상태에 영향을 미칠 수 있으므로 시스코에서는 유지 보수 기간 중 또는 중단으로 인해 구축에 미치는 영향이 최소화되는 때에 업데이트를 수행하는 것을 **권장합니다**.

설치 방법

버전 6.0으로 업데이트 하기 전에 **반드시** FireSIGHT 시스템 버전 6.0.0 설치-전 패키지를 설치해야 합니다. 자세한 내용은 *FireSIGHT 시스템 릴리스 노트 버전 6.0.0 설치-전 패키지*를 참조하십시오.

Firepower Management Center 웹 인터페이스를 사용하여 업데이트를 수행합니다. 먼저 Firepower Management Center를 업데이트한 다음 해당 관리되는 디바이스를 업데이트합니다.

설치 순서

먼저 Firepower Management Centers를 업데이트한 다음 해당 관리되는 디바이스를 업데이트합니다.

쌍으로 연결된 Firepower Management Centers에 업데이트 설치

버전 6.0에서는 고가용성 쌍에 포함된 Firepower Management Center 업데이트를 지원하지 않습니다. 고가용성 환경에서 Firepower Management Centers를 업데이트하려면 먼저 쌍을 해제한 다음 각 Firepower Management Center를 개별적으로 업데이트해야 합니다. 버전 6.0으로 업데이트하려면 고가용성 쌍을 해제해야 합니다.

클러스터링된 디바이스에 업데이트 설치

클러스터링된 디바이스(버전 6.0에서 7000 Series 또는 8000 Series 디바이스나 고가용성 쌍에 포함된 디바이스 스택)에 업데이트를 설치하면 시스템에서는 한 번에 하나씩 업데이트를 수행합니다. 업데이트가 시작되면 시스템은 한 번에 하나씩 업데이트를 수행합니다.

스태킹된 디바이스에 업데이트 설치

스태킹된 디바이스에 업데이트를 설치하면 시스템은 동시에 업데이트를 수행합니다. 업데이트가 완료되면 각 디바이스에서 정상 운영이 다시 시작됩니다. 다음을 참고하십시오.

- 모든 보조 디바이스보다 먼저 기본 디바이스가 업데이트를 완료하는 경우, 모든 디바이스에서 업데이트가 완료될 때까지 스택이 제한된 혼합- 버전 상태에서 운영됩니다.
- 모든 보조 디바이스 이후 기본 디바이스가 업데이트를 완료하는 경우, 기본 디바이스에서 업데이트가 완료되면 스택에서 정상 운영이 다시 시작됩니다.

설치 이후

Firepower Management Center 또는 관리되는 디바이스에서 업데이트를 수행한 다음에는 **반드시** 구성을 재구축해야 합니다. 구축을 수행하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*를 참조하십시오.

어플라이언스가 제대로 작동하는지 확인하려면 업데이트-뒤에 몇 가지 추가 단계를 수행해야 합니다. 예를 들면 다음과 같습니다.

- 업데이트가 성공했는지 확인
- 구축의 모든 어플라이언스가 성공적으로 통신하는지 확인
- 패치를 사용할 수 있는 경우 최신 버전 6.0 패치로 업데이트하여 최신 강화된 기능과 보안 수정 사항 적용
- (선택 사항) 침입 규칙 및 VDB(Vulnerability Database) 업데이트, 구성 재구축
- 새로운 기능, 5페이지의 정보를 기반으로 하여 필요한 구성 변경 적용

다음 섹션에서는 업데이트 수행 및 업데이트-이후 단계에 대한 자세한 지침이 제공됩니다. 반드시 명시된 작업을 모두 수행하십시오.

Firepower Management Centers 업데이트

주의: 버전 6.0으로 업데이트 하기 전에 반드시 FireSIGHT 시스템 버전 6.0.0 설치-전 패키지를 설치해야 합니다. 자세한 내용은 *FireSIGHT 시스템 릴리스 노트 버전 6.0.0 설치-전 패키지*를 참조하십시오.

이 섹션의 절차를 사용하여 가상 Firepower Management Center를 비롯한 Firepower Management Centers를 업데이트합니다. 버전 6.0 업데이트 시에는 Firepower Management Centers가 재부팅됩니다.

주의: Firepower Management Center를 업데이트하기 전에 관리되는 디바이스에 구성을 재구축합니다. 그러지 않으면 관리되는 디바이스의 업데이트가 실패할 수 있습니다.

주의: 업데이트 도중에는 로그인 프롬프트가 표시될 때까지 어플라이언스를 절대로 재부팅하거나 종료하지 마십시오. 업데이트의 사전-확인 시점에 시스템이 비활성화된 것으로 보일 수 있습니다. 이것은 정상적인 동작이므로 어플라이언스를 재부팅하거나 종료할 필요가 없습니다.

참고: Firepower Management Center를 버전 6.0으로 업데이트하면 기존에 어플라이언스에 있던 제거 프로그램이 모두 제거됩니다.

Firepower Management Center를 업데이트하려면:

1단계 릴리스 노트를 읽고 필요한 모든 업데이트-사전 작업을 완료합니다.

참고: 업데이트를 수행하기 전에 Firepower Management Center 고가용성 쌍을 해제해야 합니다. MC750, MC1500 또는 Firepower Management Center Virtual 어플라이언스에 추가 메모리를 설치해야 할 수 있습니다. Firepower Management Center에서 `RSASSA-PSS` 서명 알고리즘을 사용하는 HTTPS 인증서 또는 2048비트보다 큰 공개 키를 사용하여 생성된 인증서를 사용하는 경우, 새 인증서를 생성하여 업로드해야 합니다. 그러지 않으면 업그레이드를 수행한 다음에 Firepower Management Center에서 사용자 인터페이스에 액세스할 수 없습니다. 자세한 내용은 시작하기 전에: 중요 업데이트 및 호환성 정보, 9페이지을(를) 참고하십시오.

2단계 다음과 같이 지원 사이트에서 업데이트를 다운로드합니다.

- Firepower Management Centers 및 Firepower Management Centers Virtual의 경우:

```
Sourcefire_3D_Defense_Center_S3_Upgrade-6.0.0-1005.sh
```

참고: 지원 사이트에서 업데이트를 직접 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우, 손상될 수 있습니다.

3단계 **System(시스템) \> Updates(업데이트)**를 선택한 다음 **Product Updates(제품 업데이트)** 탭에서 **Upload Update(업데이트 업로드)**를 클릭하여 Firepower Management Center로 업데이트를 업로드합니다. 업데이트를 찾은 다음 **Upload**를 클릭합니다.

업데이트가 Firepower Management Center로 업로드됩니다. 웹 인터페이스에 방금 업로드한 업데이트의 유형, 버전 번호 및 생성된 날짜와 시간이 표시됩니다.

4단계 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

5단계 **System(시스템) \> Monitoring(모니터링) \> Task Status(작업 상태)**를 선택하여 작업 대기열을 보고 진행 중인 작업이 없는지 확인합니다.

업데이트를 시작하기 전에 오랫동안 실행되는 작업이 모두 완료될 때까지 **기다려야 합니다**. - 시스템 업데이트가 완료되면 클러터를 줄이기 위해 Message Center에서 이러한 작업의 메시지를 제거합니다.

6단계 **System(시스템) \> Updates(업데이트)**를 선택합니다.

Product Updates(제품 업데이트) 탭이 나타납니다.

7단계 사용자가 업로드한 업데이트 옆에 있는 설치 아이콘을 클릭합니다.

Install Update(업데이트 설치) 페이지가 나타납니다.

8단계 Firepower Management Center를 선택하고 **Install(설치)**을 클릭합니다. 업데이트 설치를 확인하고 Firepower Management Center를 재부팅합니다.

업데이트 프로세스가 시작됩니다. 작업 대기열에서 업데이트 진행 상황의 모니터링을 시작할 수 있습니다(**System(시스템) \> Monitoring(모니터링) \> Task Status(작업 상태)**). Firepower Management Center에서 필요한 사전-업데이트 점검을 완료하면 사용자가 로그아웃됩니다. 다시 로그인하면 Upgrade Status(업그레이드 상태) 페이지가 나타납니다. Upgrade Status(업그레이드 상태) 페이지에 진행률 표시줄이 표시되고, 현재 실행 중인 스크립트에 대한 정보가 나타납니다.

어떤 이유로든 업데이트가 실패하면, 실패 시간 및 날짜, 업데이트가 실패했을 때 실행 중이었던 스크립트, 그리고 Support(지원팀)에 문의하는 방법에 대한 지침을 나타내는 오류 메시지가 페이지에 표시됩니다. 업데이트를 다시 시작하지 **마십시오**.

주의: 업데이트에서 문제가 발생하면(예: Update Status(업데이트 상태) 페이지를 수동으로 새로 고친 후 몇 분이 흘러도 진행 상황이 표시되지 않음) 업데이트를 재시작하지 마십시오. 대신, 고객 지원에 문의하십시오.

업데이트가 완료되면 Firepower Management Center에서 성공 메시지를 표시한 후 재부팅됩니다.

9단계 업데이트가 완료되면 브라우저 캐시를 지우고 브라우저를 강제로 다시 로드합니다. 이렇게 하지 않으면 사용자 인터페이스에서 예기치 않은 동작이 발생할 수 있습니다.

10단계 Firepower Management Center에 로그인합니다.

11단계 EULA(최종 사용자 라이센스 계약)를 검토하고 수락합니다. EULA를 수락하지 않으면 어플라이언스에서 로그아웃됩니다.

12단계 **Help(도움말) \> About(정보)**을 선택하고 소프트웨어 버전이 버전 6.0으로 올바르게 표시되는지 확인합니다. Firepower Management Center에서 침입 규칙 업데이트 및 VDB의 버전도 확인하십시오. 이 정보는 나중에 필요합니다.

13단계 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

14단계 지원 사이트에서 사용 가능한 규칙 업데이트가 Firepower Management Center의 규칙보다 새로운 것이면 더 새로운 규칙을 가져옵니다. 이 시점에는 가져온 규칙을 자동-적용하지 마십시오.

규칙 업데이트 대한 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*를 참조하십시오.

15단계 지원 사이트에서 사용 가능한 VDB가 Firepower Management Center의 VDB보다 새로운 것이면 최신 VDB를 설치합니다.

VDB 업데이트를 설치하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*를 참조하십시오.

16단계 모든 관리되는 디바이스에 컨피그레이션을 재구축합니다.

구축을 수행하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*를 참조하십시오.

17단계 지원 사이트에서 버전 6.0 패치를 사용할 수 있는 경우 에 설명된 대로 해당 버전의 최신 버전을 적용합니다.

최신 강화된 기능과 보안 수정 사항을 적용하려면 최신 패치로 업데이트**해야 합니다**.

관리되는 디바이스 및 ASA FirePOWER 모듈 업데이트

Firepower Management Centers를 버전 6.0으로 업데이트한 후 이를 사용하여 해당 관리되는 디바이스를 업데이트하십시오.

주의: **버전 5.4.0.5 이하를 실행 중인 관리되는 디바이스를 보유한 시스템을 버전 6.0으로 업데이트하면 트래픽 중단 및 시스템 문제가 발생할 수 있습니다. 버전 6.0으로 업데이트하기 전에 반드시 관리되는 디바이스를 버전 5.4.0.6 이상으로 업데이트하십시오.**

자체 웹 인터페이스가 없는 관리되는 디바이스를 업데이트하려면 버전 6.0을 실행 중인 Firepower Management Center를 사용해야 합니다. ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X 또는 ASA 5516-X에서 실행 중인 ASA FirePOWER 모듈의 경우에는 Firepower Management Center를 사용하여 모듈을 업데이트하거나 ASA 디바이스에 연결한 다음 ASDM을 통해 Local Management를 사용하여 ASA FirePOWER 모듈을 업데이트할 수 있습니다. 자세한 내용은 *Cisco ASA with FirePOWER Services Local Management 릴리스 노트*를 참조하십시오.

관리되는 디바이스의 업데이트는 2-단계 프로세스입니다. 먼저, 지원 사이트에서 업데이트를 다운로드한 후 관리하는 Firepower Management Center로 업로드합니다. 그런 다음 소프트웨어를 설치합니다. 디바이스에서 동일한 업데이트 파일을 사용하는 경우 여러 디바이스를 한 번에 업데이트할 수 있습니다.

버전 6.0 업데이트의 경우 모든 디바이스가 재부팅됩니다. 7000 Series 및 8000 Series 디바이스는 업데이트 중에 트래픽 검사, 스위칭, 라우팅, NAT, VPN 또는 관련 기능을 수행하지 **않습니다**. 디바이스가 어떻게 구성되고 구축되었는지에 따라 업데이트 프로세스에 의해 트래픽 흐름 및 링크 상태가 영향을 받을 수 있습니다. 자세한 내용은 업데이트 도중 트래픽 흐름 및 검사, 11페이지을(를) 참고하십시오.

주의: **관리되는 디바이스를 업데이트하기 전에 관리되는 디바이스에 관리하는 Firepower Management Center를 사용하여 컨피그레이션을 재구축합니다. 그러지 않으면 관리되는 디바이스의 업데이트가 실패할 수 있습니다.**

주의: **업데이트 도중에는 로그인 프롬프트가 표시될 때까지 어플라이언스를 절대로 재부팅하거나 종료하지 마십시오. 업데이트의 사전-확인 시점에 시스템이 비활성화된 것으로 보일 수 있습니다. 이것은 정상적인 동작이므로 어플라이언스를 재부팅하거나 종료할 필요가 없습니다.**

관리되는 디바이스 및 ASA FirePOWER 모듈를 업데이트하려면

1단계 릴리스 노트를 읽고 필요한 모든 업데이트-사전 작업을 완료합니다.

자세한 내용은 시작하기 전에: 중요 업데이트 및 호환성 정보, 9페이지을(를) 참고하십시오.

클러스터링된 디바이스에 업데이트 설치

클러스터링된 디바이스(버전 6.0에서 7000 Series 또는 8000 Series 디바이스나 고가용성 쌍에 포함된 디바이스 스택)에 업데이트를 설치하면 시스템에서는 한 번에 하나씩 업데이트를 수행합니다. 업데이트가 시작되면 시스템은 한 번에 하나씩 업데이트를 수행합니다.

스태킹된 디바이스에 업데이트 설치

스태킹된 디바이스에 업데이트를 설치하면 시스템은 동시에 업데이트를 수행합니다. 업데이트가 완료되면 각 디바이스에서 정상 운영이 다시 시작됩니다. 다음을 참고하십시오.

- 모든 보조 디바이스보다 먼저 기본 디바이스가 업데이트를 완료하는 경우, 모든 디바이스에서 업데이트가 완료될 때까지 스택이 제한된 혼합- 버전 상태에서 운영됩니다.
- 모든 보조 디바이스 이후 기본 디바이스가 업데이트를 완료하는 경우, 기본 디바이스에서 업데이트가 완료되면 스택에서 정상 운영이 다시 시작됩니다.

설치 이후

Firepower Management Center 또는 관리되는 디바이스에서 업데이트를 수행한 다음에는 **반드시** 구성을 재구축해야 합니다. 구축을 수행하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*를 참조하십시오.

어플라이언스가 제대로 작동하는지 확인하려면 업데이트-뒤에 몇 가지 추가 단계를 수행해야 합니다. 예를 들면 다음과 같습니다.

- 업데이트가 성공했는지 확인
- 구축의 모든 어플라이언스가 성공적으로 통신하는지 확인
- 패치를 사용할 수 있는 경우 최신 버전 6.0 패치로 업데이트하여 강화된 최신 기능과 보안 수정 사항 적용
- (선택 사항) 침입 규칙 및 VDB(Vulnerability Database) 업데이트, 컨피그레이션 재구축
- 새로운 기능, 5페이지의 정보를 기반으로 하여 필요한 컨피그레이션 변경 적용

다음 섹션에서는 업데이트 수행 및 업데이트-이후 단계에 대한 자세한 지침이 제공됩니다. 반드시 명시된 작업을 모두 수행하십시오.

Firepower Management Center 업데이트

주의: **버전 6.0으로 업데이트 하기 전에 반드시 FireSIGHT 시스템 버전 6.0.0 설치-전 패키지를 설치해야 합니다. 자세한 내용은 *FireSIGHT 시스템 릴리스 노트 버전 6.0.0 설치-전 패키지*를 참조하십시오.**

이 섹션의 절차를 사용하여 가상 Firepower Management Center를 비롯한 Firepower Management Centers를 업데이트합니다. 버전 6.0 업데이트 시에는 Firepower Management Centers가 재부팅됩니다.

주의: **Firepower Management Center를 업데이트하기 전에 관리되는 디바이스에 구성을 재구축합니다. 그러지 않으면 관리되는 디바이스의 업데이트가 실패할 수 있습니다.**

해결된 문제

Cisco Bug Search Tool(https://tools.cisco.com/bugsearch/)을 사용하여 이 릴리스에서 해결된 결함을 확인할 수 있습니다. Cisco 계정이 필요합니다.

아래의 문제들은 버전 6.0에서 해결되었습니다.

- 보안 문제 CSRF(Cross-Site Request Forgery) 취약성이 해결되었습니다.
- 보안 문제 권한 있는 사용자가 경로 횡단을 사용하여 시스템 파일에 액세스할 수 있도록 하는 취약성이 해결되었습니다.
- 보안 문제 CVE-2015-0737, CVE-2015-4270, CVE-2015-6353에 기술된 사항을 포함하여 여러 XSS(Cross-Site Scripting) 취약성이 해결되었습니다.
- 보안 문제 CVE-2015-0707에 기술된 사항을 포함하여 여러 XSS(Cross-Site Scripting) 및 임의 HTML 주입 취약성이 해결되었습니다.
- 보안 문제 CVE-2010-3614, CVE-2014-3569, CVE-2014-3570, CVE-2014-3572, CVE-2014-6568, CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296, CVE-2014-9297, CVE-2014-9298, CVE-2015-0205, CVE-2015-0287, CVE-2015-0292, CVE-2015-0374, CVE-2015-0381, CVE-2015-0382, CVE-2015-0385, CVE-2015-0391, CVE-2015-0409, CVE-2015-0411, CVE-2015-0432, CVE-2015-0498, CVE-2015-0505, CVE-2015-0506, CVE-2015-0507, CVE-2015-0511, CVE-2015-1798, CVE-2015-1799, CVE-2015-1499, CVE-2015-2566, CVE-2015-2567, CVE-2015-3405, CVE-2015-3676에 기술된 MYSQL, DNS, NTP 및 OpenSSL의 여러 취약성 문제가 해결되었습니다.
- 보안 문제 CVE-2009-0696, CVE-2011-1155, CVE-2012-0876, CVE-2012-2807, CVE-2012-287, CVE-2012-3509, CVE-2012-3400, CVE-2012-3480, CVE-2012-5134, CVE-2013-0242, CVE-2013-1914, CVE-2013-4332, CVE-2013-4458, CVE-2014-3512, CVE-2014-3571, CVE-2014-3660, CVE-2014-6040, CVE-2014-8502, CVE-2015-0206, CVE-2015-0286, CVE-2015-0288, CVE-2015-0293, CVE-2015-1473, CVE-2015-1781, CVE-2015-1819에 기술된 MYSQL, Linux, GNU C Library, NTP, XML, OpenSSL 및 기타 서드파티에서 서비스 거부를 유발한 여러 취약성 문제가 해결되었습니다.
- 보안 문제 CVE-2008-3075, CVE-2008-4101, CVE-2010-2252, CVE-2010-4494, CVE-2010-4651, CVE-2011-2716, CVE-2011-3102, CVE-2014-047, CVE-2014-4877, CVE-2014-5119, CVE-2014-7817, CVE-2015-1472, CVE-2015-6307에 기술된 권한 없는 원격 공격자가 기능을 악용하거나 덮어쓸 수 있도록 하는 여러 임의 스크립트 주입 취약성이 해결되었습니다.
- 보안 문제 CVE-2012-1033 및 CVE-2015-0706에 기술된 악의적인 웹 사이트로 사용자를 리디렉션하는 HTTP 연결 처리의 여러 취약성이 해결되었습니다.
- 보안 문제 CVE-2011-1098 및 CVE-2015-3153에 기술된 권한 없는 원격 공격자가 공격받은 시스템에서 민감한 정보를 공개할 수 있도록 하는 여러 취약성이 해결되었습니다.
- 보안 문제 CVE-2014-3556에 기술된 클라이언트 연결에 대한 외부 공격을 허용하는 SSLv3의 여러 취약성이 해결되었습니다.
- 보안 문제 CVE-2009-0025, CVE-2009-4022 및 CVE-2015-0773에 기술된 사항을 포함하여 여러 파라미터 조작 및 컨피그레이션 오류 취약성이 해결되었습니다.
- 보안 문제 CVE-2015-6307에 기술된 사항을 포함하여 관리되는 디바이스가 트래픽을 처리할 때 마이크로엔진 장애를 겪을 수 있는 여러 취약성 문제가 해결되었습니다.
- 디바이스에서 충분한 양의 트래픽을 처리하지 않으면 시스템에서 완전한 성능 그래프가 생성되지 않는 문제가 해결되었습니다. (108348/CSCze87001)
- 침입 성능 그래프에 실제 수신된 패킷 수가 아닌 수신된 최소 패킷 수가 보고되는 문제가 해결되었습니다. (124331/CSCze87003)
- `4096`보다 큰 정책 식별 번호로 정책을 구축하면 오류가 발생하는 문제가 해결되었습니다. (134385/CSCze89030)
- 활성 동적 NAT 변환의 개수가 인위적으로 제한될 수 있는 문제가 해결되었습니다. (134561/CSCze87078)

- 경우에 따라 Firepower 7000 Series 및 8000 Series 디바이스의 LCD 전면 패널 화면에 일부 소프트웨어 오류가 하드웨어 오류로 표시되는 문제가 해결되었습니다. (140386/CSCze91939)
- 시스템에 로그인 실패 횟수가 표시되지 않는 문제가 해결되었습니다. (140400/CSCze87152)
- 데이터 잘라내기 기능이 개선되었습니다. (141894/ CSCze92576)
- Firepower 7000 Series 및 8000 Series 디바이스의 링크 상태 전파 반응이 개선되었습니다. (143860/CSCze87386)
- 침입 정책이나 다른 규칙에서 사용되지 않는 변수 집합을 사용하여 액세스 컨트롤 규칙을 사용 중지하면 구축이 실패하는 문제가 해결되었습니다. (143872/CSCze87308)
- URL 필터링이 개선되었습니다. (144198/CSCze94590, 144199/CSCze94758, 144685/CSCze94805)
- 업데이트가 실패한 다음 업데이트를 다시 시도하면 설치 시에 일부 드라이브가 올바르게 마운트되지 않는 문제가 해결되었습니다. (144553/CSCze95696)
- 보고 기능이 개선되었습니다. (145102/CSCze95656)
- Discovery Statistics(조회 통계) 페이지에서 통계 요약 중 **Total Events(총 이벤트)**, **Total Events Last Hour(지난 1시간 동안의 총 이벤트)** 또는 **(어제 하루 동안의 총 이벤트)** 행에 이벤트가 포함되지 않는 문제가 해결되었습니다. (145153/CSCze95751)
- Firepower 7000 Series 및 8000 Series 디바이스의 트러블슈팅이 개선되었습니다. (145187/CSCze95510)
- 시스템에서 URL 필터링 라이센스를 제거하면 클라우드 연결에 이상이 생기는 문제가 해결되었습니다. (144578/CSCze95183)
- 메모리 사용량 상태 모니터에서 허위 알림을 방지하기 위해 사용되는 계산이 수정되었습니다. (144593/CSCze94840)
- Firepower 7000 Series 디바이스의 수동 인터페이스에서 올바르지 않은 이그레스(egress) 보안 영역 및 인터페이스를 보고하는 문제가 해결되었습니다. (144624/CSCze95206)
- Object Management(개체 관리) 페이지에서 인터페이스 보안 영역을 수정하면 스태킹된 디바이스 컨피그레이션이 최신-상태가 아님에도 최신 상태로 표시되는 문제가 해결되었습니다. (144626/CSCze94847)
- Firepower 7000 Series 또는 8000 Series 디바이스의 클러스터나 디바이스 스택에 구축할 때 클러스터링된 디바이스나 스택된 디바이스에 최근 적용된 정책보다 -오래된-정책이 포함되어 있는 경우 기본 시스템이 디바이스에만 구축하는 문제가 해결되었습니다. (144646/CSCze95167)
- HTML 보고서를 생성할 때 웹 브라우저에서 보고서가 바이너리 데이터로 잘못 표시되는 문제가 해결되었습니다. (144737/CSCze95180, 144738/CSCze95205)
- 해독된 SSL 세션에서 연결 로그의 URL이 https://가 아닌 http://로 표시되는 문제가 해결되었습니다. (144785/CSCze95781)
- 기본 변수와 이름이 같지만 대소문자가 다르게 사용된 사용자 설정 네트워크 변수를 생성할 경우, 시스템에서 사용자 설정 변수와 기본 변수가 같다고 간주하고 사용자 설정 변수를 삭제하지 못하도록 하는 문제가 해결되었습니다. (44788/CSCze96160)
- 시스템에서 DNS 트래픽을 OpenVPN, QQ 및 Viber 트래픽으로 취급하는 문제가 해결되었습니다. (144789/CSCze96154)
- 공유 레이어를 참조하는 정책을 가져오면 가져오기가 실패하는 문제가 해결되었습니다. (144946/CSCze96151)
- 디스크 공간 사용률이 개선되었습니다. (145012/CSCze95309)
- Firepower 7000 Series 및 8000 Series 디바이스에서 하드웨어 엑셀러레이션(Hardware Acceleration)의 안정성이 개선되었습니다. (145035/CSCze95433, 145509/CSCze95994, CSCus68624, CSCut53335, CSCut80043)
- 규칙 문서를 볼 때 침입 규칙 편집기에서 로컬 규칙을 수정하면 시스템에서 해당 규칙을 트리거한 규칙 컨피그레이션이 아닌 이미-생성된 이벤트 데이터의 현재 로컬 규칙 컨피그레이션을 표시하는 문제가 해결되었습니다. (145118/CSCze95346)
- 시간 범위를 **지난 한 시간**으로 설정하고 침입 이벤트 성능 그래프를 생성하면 시스템에서 빈 그래프를 생성하는 문제가 해결되었습니다. (145237/CSCze95774)

- 원격 스토리지를 사용 설정하고 Firepower Management Center에서 이메일 알림 응답의 일정을 설정한 경우 일정이 설정된 이메일 알림에 의해 원격 스토리지가 사용 중지되고 원격 스토리지 백업이 실패하는 문제가 해결되었습니다. (145288/CSCze95993)
- IoC(Indication of Compromise)의 첫 번째 또는 마지막 이벤트를 보려고 할 때 시스템에서 해당 이벤트를 찾지 못하는 문제가 해결되었습니다. (145486/CSCze95786)
- 40GB 파이버 NetMod 트래픽 통계에서 잘못된 40GB 포트의 트래픽을 잘못 로깅하는 문제가 해결되었습니다. (145515/CSCze95830)
- 네트워크 사용자가 주소 표시줄에 대문자가 포함된 URL을 입력하면 웹 애플리케이션 조건이 포함된 액세스 컨트롤 규칙을 기준으로 트래픽이 확인되지 않는 문제가 해결되었습니다. (CSCur37364)
- 올바르지 않은 하위 유형 때문에 파일 경로 페이지가 로드되지 않는 문제가 해결되었습니다. (CSCur38623)
- 경우에 따라 URL 범주나 URL 평판 정보를 가져올 수 없는 문제가 해결되었습니다. (CSCur38971)
- 트래픽 프로필을 삭제하기 전에 비활성화하지 않으면 삭제된 프로필이 계속해서 리소스를 사용하는 문제가 해결되었습니다. (CSCur48345)
- 사용자 지정 워크플로를 생성하여 침입 이벤트의 패킷 보기를 열려고 하면 시스템에서 패킷 보기에 잘못된 침입 이벤트를 표시하는 문제가 해결되었습니다. (CSCur48743)
- 경우에 따라 액세스 컨트롤 정책을 수정할 수 없고 시스템에서 `Unknown Error (9999): Couldn\qt get a lock on /var/tmp/.ac_lock` 오류 메시지를 생성하는 문제가 해결되었습니다. (CSCur55338)
- 이미 새로운 버전의 VDB를 실행 중인 Firepower Management Center에서 해당 버전의 VDB(취약성 데이터베이스)를 설치하는 예약된 작업을 생성하면 시스템이 VDB를 다시 설치하고 작업이 예약될 때마다 활성 모드에서 대기 모드로 전환되는 문제가 해결되었습니다. (CSCur59252)
- 침입 이벤트나 연결 이벤트가 발생하면 트리거할 상관관계 규칙을 만든 경우 인그레스 보안 영역, 이그레스 보안 영역, 인그레스 인터페이스 또는 이그레스 인터페이스 조건이 일치하면 시스템에서 규칙을 인식하지 못하고 규칙과 일치하는 트래픽의 이벤트를 생성하는 데 실패하는 문제가 해결되었습니다. (CSCur59840)
- Firepower 7000 Series 및 8000 Series 관리되는 디바이스가 재부팅될 때 바이패스가-사용 설정된 인라인 집합에서 시스템이 25초간 인라인 연결을 유실하는 문제가 해결되었습니다. (CSCur64678)
- 이제 세션 종료 로깅을 사용 중지하여 필요한 디스크 공간을 줄일 수 있습니다. (CSCur73008)
- Network Map(네트워크 맵)의 취약성 탭에서 클라이언트 애플리케이션에 따라 취약성을 확장하면 시스템에 관련 호스트가 표시되지 않는 문제가 해결되었습니다. (CSCur86191)
- 클러스터링된 Firepower 7000 Series 또는 8000 Series 관리되는 디바이스에서 프라이빗 IP 주소 및 SFRP(시스코 Redundancy Protocol) IP 주소 양쪽으로 라우팅된 인터페이스를 구성했을 때 시스템에서 기본 IP 주소를 인식하지 못하여 OSPF(Open Shortest Path First) 연결이 설정되지 않는 문제가 해결되었습니다. (CSCur86355)
- User Preferences(사용자 환경 설정) 페이지의 Time Zone Preference(표준 시간대 환경 설정) 탭에서 표준 시간대를 변경하면 시스템에 일광 절약 시간이 포함되지 않는 문제가 해결되었습니다. (CSCur92028)
- 시스템에 대규모 데이터베이스가 포함된 경우 시스템에서 완전한 트러블슈팅 파일이 생성되지 않는 문제가 해결되었습니다. (CSCur97450)
- 액세스 컨트롤 규칙 작업 중 하나가 **Block(차단)** 또는 **Interactive Block(대화형 차단)**으로 설정되었을 때 경우에 따라 호스트에 차단 페이지가 표시되지 않는 문제가 해결되었습니다. (CSCus06868)
- 시스템이 Intrusion Policy(침입 정책) 페이지에서 등록된 대상의 수를 올바르지 않게 중복하는 문제가 해결되었습니다. (CSCus08840)
- Snort 재시작 시 시스템에서 종종 레이턴시가 발생하는 문제가 해결되었습니다. (CSCus11068)
- 모니터-전용 모드로 구성된 ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X 또는 ASA 5555-X 디바이스가 다량의 트래픽을 처리하는 경우 장애 조치를 겪게 되는 문제가 해결되었습니다. (CSCus15229)
- 시스템에서 Windows 파일 공유(SMB)를 사용할 때 보고서 이름에 지원되지 않는 문자가 포함되기 때문에 여러 보고서 유형의 생성을 지원하지 않는 문제가 해결되었습니다. (CSCus21871)

- DNS 항목 없이 도메인 이름을 구성하면 웹 인터페이스 페이지가 로드되지 않는 문제가 해결되었습니다. (CSCus28155, CSCut89714)
- 침입 정책을 수정하면 침입 규칙 가져오기가 실패하는 문제가 해결되었습니다. (CSCus29526)
- 기본 동작이 **Do Not Decrypt(해독하지 않음)**로 설정된 SSL 정책을 생성한 다음 세션 설정을 시도하면 시스템에서 해당 세션이 차단되었다고 잘못 보고하는 문제가 해결되었습니다. (CSCus41127)
- 시스코 IOS Null Route 인스턴스에 시스코 IOS 리미디에이션을 추가하고 라우터에 로그인하기 위해 암호를 입력하면 디바이스에서 암호를 받아들이지 않고 리미디에이션이 실패하는 문제가 해결되었습니다. (CSCus45769)
- 특정 이벤트 워크플로의 최적화가 개선되었습니다. (CSCus52203)
- 침입 정책이 어느 정도로 복잡한 구성을 갖는 경우 시스템이 구성의 뒷부분을 잘라서 침입 정책 구축이 실패하는 문제가 해결되었습니다. (CSCus53911)
- 메모리 사용률이 개선되었습니다. (CSCus59008, CSCuu38535, CSCuu81679)
- **Block Malware(악성코드 차단)** 규칙이 웹 애플리케이션 조건을 포함하는 액세스 컨트롤 규칙 뒤에 배치된 파일 정책을 참조하는 액세스 컨트롤 규칙을 생성하면 시스템에서 악성코드 파일을 식별하지 못하는 문제가 해결되었습니다. (CSCus64393, CSCus6452)
- 등록된 ASA FirePOWER 모듈의 암호에 지원되지 않는 문자가 포함된 경우 시스템에서 `Internal Server Error`(내부 서버 오류) 메시지가 생성되는 문제가 해결되었습니다. (CSCus68604)
- 악성코드 차단과 SSL 해독을 모두 구성하면 파일에 악성코드가 포함되어 있지 않더라도 HTTPS를 통해 파일을 다운로드할 수 없는 문제가 해결되었습니다. (CSCus72505)
- Firepower Management Centers와 관리되는 디바이스간의 통신이 개선되었습니다. (CSCus79643)
- 이제 Firepower Management Center에서 등록된 Firepower 7030 디바이스로 SSL 정책과 URL 범주 조건이 모두 포함된 액세스 컨트롤 정책을 구축할 수 있습니다. (CSCut02823)
- 네트워크 맵에서 호스트를 삭제하면 시스템이 레이턴시를 겪는 문제가 해결되었습니다. (CSCut02913)
- 상관관계 이벤트 테이블의 잘림 기능이 개선되었습니다. (CSCut02984)
- Spero 분석과 파일 캡처가 사용 설정된 파일 정책을 생성한 경우 시스템에서 수신 트래픽에서 탐지된 파일을 캡처하지 못하는 문제가 해결되었습니다. (CSCut06837)
- Windows 네트워크 파일 서버(NFS)에 위치한 백업 아카이브를 복원하는 경우 백업 복원이 실패하는 문제가 해결되었습니다. (CSCut08317)
- **Inspect Local Router Traffic(로컬 라우터 트래픽 검사)**이 사용 설정된 관리되는 디바이스에서 SSL 정책을 참조하는 액세스 컨트롤 정책을 구축하면 시스템에서 오류와 예기치 못한 문제가 발생하는 문제가 해결되었습니다. (CSCut12631)
- 디바이스 클러스터(버전 6.0에서는 고가용성이라 불림)로 구축하면 시스템이 장애 조치되지 않아야 하는 경우에도 장애 조치되는 문제가 해결되었습니다. (CSCut12919)
- 외부 시스템 로그 서버로 연결 이벤트를 보내도록 구성한 액세스 컨트롤 규칙을 생성했는데 해당 규칙이 과도하게 많은 양의 트래픽과 일치하는 경우, 관리되는 디바이스가 외부 시스템 로그 서버로의 이벤트 전송을 중단하는 문제가 해결되었습니다. (CSCut14629)
- 침입 정책 레이어가 동일한 이름을 공유하는 경우 시스템 업데이트를 수행하면 시스템에 문제가 발생하는 문제가 해결되었습니다. (CSCut16772)
- 이메일 이력 및 eStreamer 이벤트 처리 시 네트워크 매핑 생성이 개선되었습니다. (CSCut23688)
- 여러 URL 범주를 갖는 액세스 컨트롤 규칙을 수정한 다음 조건 중 하나를 제거하려고 시도하면 시스템에서 첫 번째로 나열된 범주 조건만 제거하는 문제가 해결되었습니다. (CSCut25082)
- 경우에 따라 Firepower Management Center에 시스템 문제가 발생하여 액세스 컨트롤 규칙을 로드하지 못하는 문제가 해결되었습니다. (CSCut30047)
- Firepower 8000 Series 디바이스에 수동 영역을 생성하고 `show fastpath-rules` CLI 명령을 실행하면 시스템이 침입 규칙을 비활성화된 것으로 보고하는 문제가 해결되었습니다. (CSCut32479)

- 백업 및 복원의 안정성이 개선되었습니다. (CSCut34456)
- **Inspect traffic during policy apply(정책 적용 도중 트래픽 검사)**를 사용하지 않고 구축하면 시스템에서 `Having Inspect traffic during policy apply disabled may cause network disruptions until deployment completes (정책 적용 도중 트래픽 검사를 사용 중지하면 구축이 완료될 때까지 네트워크가 중단될 수 있습니다)` 경고를 생성합니다. (CSCut36078)
- **Inspect Archives(아카이브 검사)**를 수행하도록 구성된 파일 정책을 생성하면 시스템에서 문제가 발생하고 트래픽 처리가 중단되는 문제가 해결되었습니다. (CSCut39253, CSCuu14892)
- 침입 이벤트 테이블 보기에서 검토나 복사하기 위해 하나 이상의 Original Client IP 열의 셀을 선택하면 시스템에서 오류가 생성되고 선택한 행이 표시되지 않는 문제가 해결되었습니다. (CSCut41458)
- 다수의 액세스 컨트롤 대상 사용자가 포함된 LDAP 그룹에서 사용자들을 대상으로 액세스-컨트롤 규칙을 만들면 시스템에서 레이턴시가 발생하고 트래픽을 일치시키지 않는 문제가 해결되었습니다. (CSCut56233)
- 생성된 이벤트의 검색을 생성 및 수정한 다음 검색이 시작하기 전에 취소하면 시스템에서 올바르지 않은 검색 이름을 가진 검색과 관련된 이벤트 페이지로 사용자를 리디렉션하는 문제가 해결되었습니다. (CSCut63265)
- 디스크 관리자 기능이 개선되었습니다. (CSCut65740)
- 맵 목록에 있는 마지막 항목이 중복 항목인 경우 시스템에서 문제가 발생하는 문제가 해결되었습니다. (CSCut65738)
- 침입 규칙 업데이트를 가져오면 시스템에서 문제가 발생하는 문제가 해결되었습니다. (CSCut65772)
- 경우에 따라 시스템이 데이터베이스 통신을 폐기하고 오류가 발생하는 문제가 해결되었습니다. (CSCut71816)
- 고-가용성 쌍에서 등록된 Firepower 7000 Series 및 8000 Series 디바이스로 Firepower Management Center에 구축하면 경우에 따라 장애 조치가 발생하는 문제가 해결되었습니다. (CSCut72278)
- Cloud Lookup(클라우드 조회) 장애 조치의 상태 경고 알림이 개선되었습니다. (CSCut77594)
- 시스템에서 연속해서 두 번 장애가 발생하면 바이패스 모드가 사용 설정되지 않았더라도 시스템이 바이패스 모드로 전환되는 문제가 해결되었습니다. (CSCut80892)
- Retrospective Malware Events(이전 악성코드 이벤트) 테이블 보기의 메시지 열에 이전 악성코드 이벤트의 구 특성값이나 신규 특성값이 포함되지 않는 문제가 해결되었습니다. (CSCut83512)
- SFR5585-X 서비스 카드는 재시작하지 않고 다량의 하위 인터페이스가 구성된 ASA 5585-X 디바이스를 재시작하는 경우 SFR5585-X 서비스 카드에 장애가 발생한 것처럼 보이는 문제가 해결되었습니다. (CSCut89619)
- 여러 인터페이스가 구성된 시스템에 등록된 디바이스에서 `show managers` CLI 명령을 사용하면 시스템에 올바르지 않은 IP 주소가 표시되는 문제가 해결되었습니다. (CSCut95947)
- 경우에 따라 업데이트 실패가 제시간에 파악되지 않는 문제가 해결되었습니다. (CSCuu01055)
- 시스템 문제가 발생하면 클라우드에서 새로운 업데이트가 있는지 계속해서 확인하는 문제가 해결되었습니다. (CSCuu04844)
- URL 범주 조건이 있는 액세스 컨트롤 정책을 생성했는데 네트워크 맵에서 완전한 데이터베이스가 로드되지 못한 경우 시스템에서 문제가 발생하는 문제가 해결되었습니다. (CSCuu06714)
- VDB(vulnerability database, 취약성 데이터베이스) 설치에 예상보다 긴 시간이 걸리는 문제가 해결되었습니다. (CSCuu06786)
- 경우에 따라 Firepower Management Center가 등록된 디바이스로부터 상태 이벤트 수신을 받지 않는 문제가 해결되었습니다. (CSCuu18450)
- Cisco Nexus 7000 스위치에 연결된 상태로 Firepower 7000 Series 또는 8000 Series 디바이스에서 LAG(Link Aggregation Group)를 생성하면 시스템에서 레이턴시가 발생하는 문제가 해결되었습니다. (CSCuu31626)
- 시스템 표준 시간대를 UTC+ 구역으로 바꾸고 적어도 하나의 비활성 기간을 갖는 상관관계 규칙을 상관관계 정책에 추가한 경우 상관관계 규칙을 활성화해도 활성화되지 않는 문제가 해결되었습니다. (CSCuu37600)
- 클러스터링된 Firepower 7000 Series 또는 8000 Series 디바이스(버전 6.0에서는 고가용성이라 불림)에서 라우팅된 인터페이스를 생성하면 연결 문제가 발생하는 문제가 해결되었습니다. (CSCuu37668)

- 라우팅된 IP 주소를 추가하거나 수정하면 SFRP(시스코 이중화 프로토콜) 광고값이 구성 가능하지 않음에도 구성 가능한 것으로 표시되는 문제가 해결되었습니다. (CSCuu37687)
- 둘 이상의 관리 인터페이스가 사용 설정된 상태에서 한 인터페이스의 웹 클라이언트 연결이 끊긴 경우 시스템이 올바르지 않은 게이트웨이 IP 주소로 변경되어 인터페이스에 액세스할 수 없게 되는 문제가 해결되었습니다. (CSCuu44020)
- 위치 정보 조건을 갖는 액세스 컨트롤 정책을 생성한 경우 조건과 일치해야 하는 트래픽이 일치하지 않는 문제가 해결되었습니다. (CSCuu48800)
- 네트워크 맵 생성이 개선되었습니다. (CSCuu53215, CSCuu94784, CSCuv72386, CSCuw06359)
- 액세스 컨트롤 정책에서 수동 URL 조건을 갖는 액세스 컨트롤 규칙 참조 시 로드 시간이 개선되었습니다. (CSCuu55853)
- 최소 ASA 버전 9.3.2.2 이상을 실행 중인 ASA Firepower 모듈(ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X)에서 mpf-policy-map-class 모드가 실행되지 않는 문제가 해결되었습니다. (CSCuu68273)
- 무효화된 서브넷 IP 주소를 사용하는 오리지널 클라이언트 IP를 갖는 침입 이벤트를 위해 검색을 생성하면 시스템이 오리지널 클라이언트 IP가 없는 침입 이벤트를 제외시키는 문제가 해결되었습니다. (CSCuu68438)
- 시스템이 드물게 안정적이 못해 보이고 재부팅 이후 복구되지 않는 문제가 해결되었습니다. (CSCuu93154)
- 일부 DC4000 어플라이언스의 드라이브에 장애가 발생하는 경우 RAID 컨트롤러에 장애가 발생하고 데이터가 손실되는 문제가 해결되었습니다. (CSCuu93159)
- eStreamer 성능이 개선되었습니다. (CSCuu94902)
- 웹 브라우저에서 비디오 스트리밍처럼 용량이-큰 미디어를 봤을 때 Summary Dashboard(요약 대시보드)의 Top Web Applications Seen(많이 본 웹 애플리케이션) 위젯과 Top Client Applications Seen(많이 본 클라이언트 애플리케이션) 위젯에 올바른 바이트 수가 표시되지 않는 문제가 해결되었습니다. (CSCuu97036)
- 관리되는 디바이스의 SSL 정책을 **Decrypt-Resign**(해독-파기)으로 설정한 경우, 하나의 인터페이스 집합에서 이그레스되어 해독된 트래픽이 스위칭 또는 라우팅되어 트래픽이 동일한 관리되는 디바이스의 다른 인터페이스 집합으로 인그레스되고 시스템의 SSL 트래픽이 중단되는 문제가 해결되었습니다. (CSCuu97712)
- 보고서를 생성한 다음 Report Templates(보고서 템플릿) 탭에서 다른 곳으로 이동한 다음 다른 보고서를 생성했을 때 Reporting(보고) 페이지의 Report Templates(보고서 템플릿) 탭에 있는 **Send email(이메일 보내기)** 체크 박스의 선택이 유지되지 않고 이메일을 통해 더 이상 보고서가 전송되지 않는 문제가 해결되었습니다. (CSCuu97750, CSCuu41580, CSCuv43116)
- 인터랙티브 차단 웹 페이지에서 **Continue(계속)**를 클릭해도 차단된 웹 페이지로 리디렉션되지 않는 경우가 발생하는 문제가 해결되었습니다. (CSCuu97934, CSCuu97946)
- 경우에 따라 업데이트가 실패하는 문제가 해결되었습니다. (CSCuu99337)
- 시스템에서 사용자들을 기본 LDAP 그룹의 구성원으로 인식하지 않는 문제가 해결되었습니다. (CSCuv03821)
- 연결 이벤트 보고서를 생성하여 **Maximum Results(최대 결과)** 값을 수정하면 시스템에서 새로운 값을 저장하지 않고 기본값을 사용하여 보고서를 생성하는 문제가 해결되었습니다. (CSCuv06557)
- 버전 5.4보다 오래된 버전을 실행 중인 관리되는 디바이스를 갖는 시스템과 시간을 동기화시키기 위해 원격 NTP 서버를 사용하도록 시스템을 구성한 상태에서 윤초가 지나가면 시스템이 다량의 CPU 리소스를 사용하는 문제가 해결되었습니다. (CSCuv11738)
- Interactive Block(대화형 차단) 조치로 구성된 액세스 컨트롤 규칙을 생성하고 Chrome 웹 브라우저에서 차단된 웹 페이지를 보는 경우, 페이지 차단을 바이패스하는 **Continue(계속)** 버튼이 작동하지 않는 문제가 해결되었습니다. (CSCuv21748)
- 생성된 내부 CA 인증서가 10년이 아닌 30일간만 유효한 문제가 해결되었습니다. (CSCuv29004)
- 호스트가 IoC(Indication of Compromise, 보안 침해 지표)를 생성하여서 사용자가 Host Profile(호스트 프로필) 페이지에서 해당 호스트의 IoC를 비활성화 경우, 호스트의 보안 침해 지표 대시보드 위젯에 IoC가 표시되지 않아야 하는 경우에도 표시되는 문제가 해결되었습니다. (CSCuv41376)

- 7000 Series 또는 8000 Series 디바이스에서 기본 동작이 **Decrypt - Known Key(해독 - 알려진 키)** 또는 **Decrypt - Resign(해독 - 파기)**으로 설정된 SSL 정책을 생성한 다음 다른 소스 IP 주소로 SSL 세션을 재개하려고 선택하면 SSL 검사가 실패하고 연결 로그에 올바르지 않은 SSL 정책 기본 동작이 표시되는 문제가 해결되었습니다. (CSCuv48689)
- 파일 탐지 및 차단 기능이 개선되었습니다. (CSCuv59181)
- 액세스 컨트롤 규칙의 포트 범위를 위한 메모리 사용률이 개선되었습니다. (CSCuv64114)
- 여러 디바이스를 등록했거나 관리되는 디바이스에서 여러 인터페이스를 구성했거나 여러 VPN 구축을 생성한 경우 시스템이 각각의 페이지에서 모든 디바이스 또는 인터페이스 또는 VPN 구축에 관한 정보를 생성하지 않는 문제가 해결되었습니다. (CSCuv76287)
- 상태 모니터 알림이 개선되었습니다. (CSCuv96121)
- 침입 정책 레이어를 병합하면 오류가 생성되는 문제가 해결되었습니다. (CSCuw34380)
- 이메일 알림의 안정성이 개선되었습니다. (CSCuw36354)
- 경우에 따라 유효하지 않은 사용자 이름 값 때문에 시스템에서 오류가 발생하는 문제가 해결되었습니다. (CSCuw39725)
- MC4000에서 SOL(Serial Over Lan)을 LOM(Lights-out-Management)으로 전환하거나 그 반대로 전환한 경우 시스템의 콘솔 포트가 작동하지 않는 문제가 해결되었습니다. (CSCuw67319)
- `system support ssl-debug` 또는 `system support debug-DAQ-NSE` CLI 명령을 사용하여 SSL 디버그 로깅을 사용 설정한 상태에서 시스템이 오랜 시간 다량의 트래픽을 경험하면 시스템에서 디스크 공간 문제가 발생하는 문제가 해결되었습니다. (CSCuw68004)
- 기본 동작이 **Malware Block(악성코드 차단)**으로 설정된 파일 정책을 구축한 뒤 시스템에서 SMB 트래픽이 탐지되면 시스템에서 문제가 발생하는 문제가 해결되었습니다. (CSCux49653)

알려진 문제

Cisco Bug Search Tool(https://tools.cisco.com/bugsearch/)을 사용하여 이 릴리스의 알려진 문제를 확인할 수 있습니다. Cisco 계정이 필요합니다.

버전 6.0에는 다음과 같은 알려진 문제들이 있습니다.

- 버전 6.0으로 업데이트 하기 전에 **반드시** FireSIGHT 시스템 버전 6.0.0 설치-전 패키지를 설치해야 합니다. 자세한 내용은 *FireSIGHT 시스템 릴리스 노트 버전 6.0.0 설치-전 패키지*를 참조하십시오.
- Firefox 버전 38.0.1을 사용하여 Firepower Management Center 인터페이스를 보면 레이턴시를 경험할 수 있습니다. 이를 해결하려면 Firefox 41 이상이나 다른 웹 브라우저를 사용하십시오. (CSCuv11830)
- 하위 도메인에 디바이스를 등록할 때 액세스 컨트롤 정책을 생성하면 시스템이 하위 도메인이 아닌 전역 도메인에 액세스 컨트롤 정책을 만드는 경우가 있습니다. (CSCut56951)
- Access Control(액세스 컨트롤) 페이지(**Policies(정책) \> Access Control(액세스 컨트롤)**)의 고급 탭에서 기본 네트워크 액세스 정책을 수정하면 시스템이 구축 대화 상자 창에 기본 네트워크 액세스 정책을 침입 정책으로 잘못 표시하는 경우가 있습니다. (CSCuv48221)
- ASDM을 통해 관리되는 ASA FirePOWER 모듈에서 Select Comparison(비교 선택) 페이지(**ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) \> Policies(정책) \> Files(파일) \> Compare Policies(정책 비교)**)에 있는 도움말 아이콘을 클릭해도 온라인 도움말이 열리지 않습니다. (CSCuw21863)
- Firepower 7000 Series 또는 8000 Series 디바이스의 Intrusion Events(침입 이벤트) 테이블 보기 페이지에서 **All Events (Not Dropped)(모든 이벤트(폐기되지 않음)**를 보고 **Review By(검토 기한)** 및 **Count(개수)**를 포함하여 최대 여섯 개의 필드로 테이블을 정렬한 다음 보고서를 생성하면 보고서가 생성되지 않습니다. 이를 해결하려면 **Review By(검토 기한)** 및 **Count(개수)** 필드 값 중 하나를 제외하거나, **Review By(검토 기한)** 및 **Count(개수)** 필드를 모두 포함해야 하면 침입 이벤트 페이지에서 보고서 생성 시 셋보다 많은 추가 필드 값을 추가하지 않습니다. (CSCuw29993)

- 시스템에서 `This field contains invalid characters. Only alphanumerics, hyphen ( - ), underscore ( _ ), period ( . ), and plus ( + ) are allowed` 메시지가 표시됨에도 불구하고 디바이스 그룹에 더하기(+) 문자가 포함된 이름을 지정할 수 없습니다. (CSCuw44373)
- Shell Timeout(셸 타임아웃) 페이지(**System(시스템) \> Configuration(컨피그레이션) \> Shell Timeout(셸 타임아웃)**)에서 브라우저 및 셸 타임아웃 임계값을 수정한 다음 재구축하면 설정된 임계값이 지난 다음 최대 1분 후에 시스템에서 활성 상태가 아닌 Firepower Management Centers에서 로그아웃하는 경우가 있습니다. (CSCuw48568)
- 도메인에 포함된 파일 목록을 수정하면 해당 도메인의 파일 정책이 최신-상태가-아닌 것으로 표시되는 경우가 있습니다. (CSCuw52764)
- Device Management(디바이스 관리) 페이지(**Devices(디바이스) \> Device Management(디바이스 관리)**)의 툴팁에 디바이스 개체에 관한 디바이스 재정의 값이 표시되지 않습니다. (CSCuw53371)
- 버전 5.4.x의 외부 인증서는 버전 6.0에서 지원되지 않습니다. 버전 6.0에서 지원되는 커브는 `prime192v1, prime256v1,secp384r1 secp521r1`로만 한정됩니다. 지원되는 외부 인증서를 획득하려면 시스템을 버전 6.0으로 업데이트해야 합니다. (CSCuw54749)
- Outlook 2013으로 이메일을 보내고 받는 시스템에서 파일 규칙이 **Detect Files(파일 탐지)**로 설정된 파일 정책과 **Decrypt--Resign(해독-파기)** 또는 **Decrypt--known key(해독-알려진 키)**로 구성된 SSL 정책을 모두 참조하는 액세스 컨트롤 정책을 생성할 때, 연결 이벤트 페이지(**Analysis(분석) \> Connections(연결) \> Events(이벤트)**)에 이메일 첨부 파일이 포함되지 않는 경우가 있습니다. (CSCuw65152)
- Device Management(디바이스 관리) 페이지(**Devices(디바이스) \> Device Management(디바이스 관리)**) 또는 NAT 페이지(**Devices(디바이스) \> NAT**) 또는 VPN 페이지(**Devices(디바이스) \> VPN**)에서 탭을 새로 고쳐도 시스템이 해당 페이지의 캐시를 지우지 않고 **Save(저장)** 버튼도 작동하지-않는 경우가 있습니다. 이를 해결하려면 해당 페이지나 탭에서 변경한 사항을 모두 취소한 다음 변경하려는 디바이스를 다시 한 번 선택합니다. (CSCuw75367)
- 만료됨 또는 철회됨 등과 같이 둘 이상의 상태를 갖는 인증서가 포함된 SSL 정책을 생성하면 Connection Events(연결 이벤트) 페이지(**Analysis(분석) \> Connections(연결) \> Events(이벤트)**)의 Certificate Status(인증서 상태) 열에 상태가 표시되지 않는 경우가 있습니다. (CSCuw76040)
- 드문 경우지만, Device Management(디바이스 관리) 페이지(**Devices(디바이스) \> Devices Management(디바이스 관리)**)에서 디바이스 인터페이스를 생성하거나 수정하면 시스템에서 `No cache exists to discard and resume(폐기 후 재개할 캐시가 존재하지 않음)` 오류가 생성되고 구축이 수행되지 않는 경우가 있습니다. 이를 해결하려면 Device Management(디바이스 관리) 페이지를 새로 고침하고 다시 구축합니다. (CSCuw77505)
- 디바이스의 가상 라우터 페이지(**Devices(디바이스) \> Devices Management(디바이스 관리) \> Virtual Router(가상 라우터)**)에서 OSPFv3, RIP 또는 BGP를 올바르지 않게 구성한 다음 변경 사항을 저장하지 않고 컨피그레이션 페이지를 나가면 시스템에서 **To revert back the configuration(컨피그레이션을 되돌리려면)** 팝-업이 생성되는 경우가 있습니다. 가상 라우터 컨피그레이션 페이지에서 변경 사항을 제거하려면 **Yes(예)**를 클릭합니다. **No(아니요)**를 클릭하면 시스템에서 **To revert back the configuration(컨피그레이션을 되돌리려면)** 팝-업을 여러 번 표시한 다음 변경 사항 없이 가상 라우터 컨피그레이션 페이지를 저장합니다. (CSCuw78916)
- 나, 클러스터링되거나 스태킹된 Firepower 7000 Series 또는 8000 Series 디바이스(버전 6.0에서는 고가용성이라 불림)에 네트워크 검색 정책을 구축하면 시스템에서 해당 클러스터나 스택의 디바이스 하나를 표시하는 대신 해당 클러스터나 스택에 포함된 모든 디바이스의 개수를 셉니다. (CSCuw79241, CSCuw79243)
- Firepower Management Center, Firepower 7000 Series 또는 8000 Series 디바이스에서 초기 설정이 끝난 다음 NAT 디바이스 뒤에 있는 어플라이언스에서 연결하는 경우, 시스템에서 사용자가 연결하려는 NAT IP가 아니라 사용자가 어플라이언스에 구성한 IP 주소를 포함하는 리디렉션 URL을 제공하고 세션이 타임아웃됩니다. 이를 해결하려면 웹을 통해 연결하는 데 사용되는 NAT IP를 사용하도록 URL을 수정합니다. (CSCuw79967)
- 버전 5.4.1.3 이상의 설치를 제거하고 이전 버전인 5.4.x 버전으로 돌아간 다음 시스템을 버전 6.0으로 업데이트하면 업데이트가 되지 않습니다. 시스템을 버전 6.0으로 업데이트하기 전에 최신 버전으로 업데이트하십시오. (CSCuw81780)
- 장비 등록 전에 디바이스의 필수 라이선스를 선택하지 않으면 시스템에서 `Initial policy deployment not started due to validation errors. For details, redeploy manually(검증 오류로 인해 초기 정책 구축이 시작되지 않았습니다. 자세한 내용이 필요하면 수동으로 재구축하십시오` 메시지가 생성되는 경우가 있습니다. 디바이스에 선택해야 하는 올바른 라이선스에 대한 자세한 내용은 *Firepower Management Center컨피그레이션 가이드*의 FireSIGHT System 라이선스 챕터를 참조하십시오. (CSCuw85743)

- Firepower 7000 Series 또는 8000 Series 관리되는 디바이스의 라우팅된 인터페이스를 대상으로 하는 규칙이 포함된 NAT 정책을 구축한 다음 관리되는 디바이스를 클러스터링하면(버전 6.0에서는 고-가용성 쌍이라 불림) 일부 NAT 규칙이 고가용성 인터페이스가 대상이 되도록 변경되는 대신 관리되는 디바이스의 라우팅된 인터페이스를 계속해서 대상으로 삼는 경우가 있습니다. 이를 해결하려면 개별 인터페이스가 포함된 규칙을 수정하고 고가용성 인터페이스를 수동으로 생성한 다음 다시 구축합니다. (CSCuw89223)
- HTTP Listing(HTTP 나열) 페이지(**Device(디바이스) \> Platform Settings(플랫폼 설정) \> Firepower Threat Defense Platform Settings(Firepower Threat Defense 플랫폼 설정) \> HTTP**)에 **Authentication Certificate(인증 인증서)**가 구성 가성한 필드로 잘못 표시됩니다. (CSCuw89605)
- 시스템에서 HTTP 전처리기 규칙에 명시되지 않은 포트에서 처리된 다량의 HTTP 트래픽을 위한 이벤트를 생성하는 경우가 있습니다. 이를 해결하려면 HTTP 전처리기 규칙에 GID `119`, SID `15`의 포트를 추가합니다. (CSCuw90033)
- Firepower Management Center를 백업하는 도중에 구축을 시작해도 통신 채널이 차단되어 정책이 구축될 수 없다는 메시지가 표시되지 않습니다. 백업 프로세스가 완료될 때까지 기다린 다음 다시 구축합니다. (CSCuw90629)
- 기본 작업이 침입 정책인 액세스 컨트롤 정책을 생성하면 기본 작업 옆에 있는 변수 집합 아이콘이 올바르게 표시되지 않는 경우가 있습니다. 이를 해결하려면 기본 작업이 다른 침입 정책을 사용하도록 변경하여 아이콘이 표시되게 한 다음 기본 작업을 기존 침입 정책으로 다시 변경합니다. (CSCuw94067)
- Firepower Management Center를 버전 6.0으로 업데이트하고 컨피그레이션 변경 내용을 구축한 뒤 Firepower Management Center의 Deploy(구축) 창에 올바르지 않은 타임스탬프가 표시되는 경우가 있습니다. (CSCuw94083)
- OSPFv3 라우터를 생성한 다음 라우터 페이지(**Devices(디바이스) \> Device Management(디바이스 관리) \> Router(라우터)**)의 Advanced Settings(고급 설정) 탭에서 수동 router-id를 구성하지 않으면 시스템에서 이름이 지정되지 않은 IPv4 IP 주소를 사용하지 않고 `구성된 라우터 ID가 없으므로 OPSFv3 라우터 프로세스가 시작되지 않습니다. Neither router ID in OSPFv3 nor IPv4 address configured in Interfaces`(라우터 `ID`가 구성되지 않았으므로 `OSPFv3` 라우터 프로세스가 시작할 수 없습니다. 인터페이스에서 `OSPFv3`과 `IPv4` 주소 모두에서 라우터 `ID`가 구성되지 않았습니다 오류 메시지가 생성됩니다. (CSCuw95485)
- **MAC Vendor is(MAC 벤더와 동일)** 조건과 일치하도록 구성된 상관관계 규칙을 만들면 시스템에서 `Warning: no vendors match this string`(경고: 이 스트링과 일치하는 벤더 없음) 경고를 생성하고 상관관계 규칙을 실행하지 않습니다. 이를 해결하려면 VDB(vulnerability database, 취약성 데이터베이스)를 업데이트합니다. VDB를 업데이트해도 문제가 해결되지 않으면 **MAC Vendor is(MAC 벤더와 동일)** 조건 대신 **MAC Vendor contains(MAC 벤더에 포함)** 조건을 사용합니다. (CSCuw96022)
- Firepower Management CenterSmart Licensing(스마트 라이선스) 사용자 인터페이스 페이지(**System(시스템) \> Local(로컬) \> System Policy(시스템 정책)**)에 있는 Cisco Smart Software Manager 링크가 업데이트된 링크로 디렉션되며, 이후 또 다시 리디렉션됩니다. 이를 해결하려면 리디렉션이 신속히 수행되지 않을 때 https://software.cisco.com/#module/SmartLicensing으로 연결합니다. (CSCuw96552)
- 악성코드 차단을 위해 구성된 파일 정책을 참조하는 액세스 컨트롤 정책을 구축하는 경우, 버전 6.0을 실행 중인 Firepower Management Center에 등록되었으며 버전 5.4.0을 실행 중인 디바이스에서 구축이 되지 않는 경우가 있습니다. (CSCuw97809)
- Intrusion Policy(침입 정책) 페이지(**Policies(정책) \> Intrusion(침입) \> Intrusion Policy(침입 정책)**)의 Advanced Settings(고급 설정)에서 민감한 데이터 탐지를 사용 설정한 다음 저장하지 않고 다른 도메인으로 전환하면 시스템에서 목적지 도메인에 Intrusion Policy(침임 정책) 페이지를 다시 로드하지 않는 경우가 있습니다. 이를 해결하려면 저장하거나 Intrusion Policy(침입 정책) 페이지를 수동으로 다시 로드합니다. (CSCuw97864)
- 버전 6.0을 실행 중인 디바이스에 구성된 시간이 Firepower Management Center에 구성된 시간보다 이른 경우, 관리되는 디바이스를 Firepower Management Center에 등록하면 해당 제품에서 연결 복구 시에 문제가 발생하는 경우가 있습니다. 이를 해결하려면 `/etc/rc.d/init.d/pm restart` CLI 명령을 실행합니다. 연결 문제가 지속되면 Support(지원팀)로 문의하십시오. (CSCuw97948)
- 버전 6.0을 실행 중인 디바이스에 구성된 시간이 Firepower Management Center에 구성된 시간보다 이른 경우, 관리되는 디바이스를 Firepower Management Center에 등록하면 연결 문제가 발생하고 시스템이 연결을 복구하지 못하는 경우가 있습니다. 이를 해결하려면 `/etc/rc.d/init.d/pm restart` CLI 명령을 실행합니다. 연결 문제가 지속되면 Support(지원팀)로 문의하십시오. (CSCuw97948)
- 사용자 인터페이스에서 복원을 시작할 때 세션 연결이 끊겨서 복원 작업의 상태를 보려면 다시 로그인해야 하는 경우가 있습니다. (CSCuw98296)

- 버전 6.0을 실행 중인 Firepower Management Center에 2개의 하위 도메인을 생성하고 7000 Series 또는 8000 Series 디바이스를 등록하고, 네트워크 개체 재정의를 생성하고 액세스 컨트롤 정책을 구축한 다음 디바이스를 하나의 하위 도메인에서 다른 하위 도메인으로 이동하면 시스템이 Object(개체) 페이지에서 재정의 값을 삭제합니다. (CSCuw98708)
- 버전 6.0은 MAC OS를 실행 중인 시스템에서 Safari 웹 브라우저를 지원하지 않습니다. Firefox, Chrome 또는 Internet Explorer를 사용하십시오. (CSCuw98876)
- 가상 디바이스를 호스팅하는 시스템이 다량의 트래픽을 경험하는 경우, 가상 디바이스에 구축하면 일시적인 네트워크 문제가 발생하는 경우가 있습니다. (CSCux00380)
- 침입 이벤트에 올바른 소스 IP 주소나 올바른 대상 IP 주소가 표시되지 않는 경우가 있습니다. 이를 해결하려면 Connection Events(연결 이벤트) 페이지(**Analysis(분석) \> Connections(연결) \> Events(이벤트)**)에서 침입 이벤트의 올바른 소스 IP 주소와 목적지 IP 주소를 확인합니다. (CSCux00385)
- SIP(Session Initiation Protocol)를 사용하는 호출에 의해 설정된 RTP(Real-time Transport Protocol)을 위해 핀홀이 생성되지 않는 경우가 있으며, 이때 해당 SIP 호출의 VOIP 채널이 생성되지 않습니다. (CSCux03758, CSCux09765)
- Skinny(SCCP) 프로토콜에서 애플리케이션 탐지기를 사용할 수 있긴 하나, SCCP 패킷에 의해 설정된 RTP 연결에는 핀홀이 생성되지 않습니다. (CSCux05468)
- 많은 수의 디바이스에 정책을 구축할 때 Snort가 재시작되지 않으면 정책 구축이 타임아웃되고 구축되지 않는 경우가 있습니다. (CSCux07861)
- 하위 도메인에 포함된 NAT 정책을 Firepower 7000 Series 또는 8000 Series 디바이스에 구축하고 디바이스를 새 도메인으로 옮기면 구축이 되지 않습니다. 이를 해결하려면 새 도메인에 새 NAT 정책을 생성하고 올바른 디바이스를 대상으로 설정한 다음 재구축합니다. (CSCux10651)
- 등록된 디바이스에서 VPN 구축을 생성하고 디바이스를 하나의 도메인에서 다른 도메인으로 옮긴 다음 구축하면 구축이 되지 않고 시스템에서 `Pre-deploy Global Configuration Generation. Cannot find policy information(배포 전에 전역 컨피그레이션 생성. 정책 정보를 찾을 수 없음)` 오류 메시지를 생성하는 경우가 있습니다. 이를 해결하려면 디바이스를 다른 도메인으로 옮기기 전에 VPN 컨피그레이션을 제거합니다. 또 다른 해결 방법으로는 등록을 해제하고 Firepower Management Center에 디바이스를 등록하고 VPN 구축을 생성한 다음 구축하는 방법이 있습니다. (CSCux10820)
- Firepower Management Center에서 RSASSA-PSS 서명 알고리즘을 가진 인증서를 사용하는 것은 버전 6.0에서 지원하지 않습니다. 이러한 인증서를 사용하는 Firepower Management Center를 버전 6.0으로 업데이트하거나 버전 6.0에 이러한 인증서를 추가하면 Management Center 웹 인터페이스에 로그인할 수 없고, 시스템에서 `Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator` 오류가 발생합니다. 이를 해결하려면 업데이트를 수행하기 전에 `sha1WithRSAEncryption` 또는 `sha256WithRSAEncryption` 알고리즘의 SSL 인증서를 생성하여 설치한 다음 Firepower Management Center를 재시작하거나 기본 Firepower Management Center 인증서를 사용한 다음 어플라이언스를 재시작하십시오. Firepower Management Center에서 사용자 인터페이스에 액세스할 수 없으면 Support(지원팀)으로 문의하십시오. (CSCux30610)
- 버전 5.4 이상을 실행 중인 관리되는 Firepower 어플라이언스에서 여러 항목을 갖는 네트워크 개체가 포함된 SSL 정책을 참조하는 액세스 컨트롤 정책을 생성하고 시스템을 버전 6.0으로 업데이트하면 버전 6.0을 실행 중인 Firepower Management Center에서 정책이 구축되지 않는 경우가 있습니다. 이를 해결하려면 시스템을 버전 6.0으로 업데이트한 다음 SSL 정책을 수정하고 네트워크 개체를 제거한 다음 네트워크 개체를 추가하고 다시 구축합니다. (CSCux31618)
- Firepower Management Center에서 되는 인증서가 2048비트보다 큰 공개 서버 키를 사용하여 생성된 경우에는 버전 6.0으로 업데이트한 뒤 Firepower Management Center 웹 인터페이스에 로그인할 수 없게 됩니다. 이를 해결하려면 서버 인증서 요청을 생성하여 인증서를 생성하고 생성된 인증서를 Firepower Management Center에 적용함으로써 크기가 큰 공개 키로 생성된 인증서를 대체합니다. 서버 인증서 요청과 인증서 업로드는 Firepower Management Center(**System(시스템) \> Local(로컬) \> Configuration(구성) \> HTTPS Certificate(HTTPS 인증서)**)에 있는 로컬 구성 설정을 통해 수행할 수 있습니다. Firepower Management Center에서 CSR을 사용하지 않고 인증서를 생성한 경우에는 2048비트 이하의 공개 키를 사용합니다. 2048비트 이상이 포함된 인증서를 생성했는데 Management Center 웹 인터페이스에 액세스할 수 없는 경우 Support(지원팀)으로 문의하십시오. (CSCux35430)
- 맞춤형 URL을 포함하는 액세스 컨트롤 정책을 구축하면 CPU 리소스가 과도하게 사용되고 시스템에서 문제가 발생하는 경우가 있습니다. (CSCux35554)

- Firepower Threat Defense를 실행 중인 디바이스가 버전 6.0을 10일 이상 실행 중인 Firepower Management Center에 등록된 경우 시스템에서 다음과 같은 문제가 발생합니다. Firepower Management Center가 새 디바이스를 등록할 때 `CSM failed state: (2) CSM can not provide device state (2)(CSM 실패 상태: (2) CSM이 디바이스 상태 (2)를 제공할 수 없음)` 오류를 생성하고 디바이스가 등록되지 않습니다. Firepower Management Center를 6.0.0에서 이후 버전으로 업데이트하면 `Installation failed. Peer discovery incomplete. Please retry after few moments(설치하지 못했습니다. 피어 검색이 완료되지 않았습니다. 잠시 후 다시 시도하십시오)` 오류가 발생하고 업데이트가 되지 않습니다. Firepower Management Center를 백업하면 `Registration or CSM state are blocking backup(등록 또는 CSM 상태가 백업을 차단하고 있음)` 오류가 발생하고 백업이 되지 않습니다. Firepower Management Center에서 도메인의 생성, 업데이트 또는 삭제를 시도하면 `sensor registration process is running. Please wait until process completes.` 오류가 생성되고 시스템에서 도메인이 성공적으로 생성, 업데이트 또는 삭제되지 않습니다. 이를 해결하려면 Firepower Management Center에서 버전 6.0 설치 파일을 다운로드하고 루트 사용자 권한으로 `/usr/local/sf/bin/install_update.pl /var/sf/updates/[UPGRADE_PKG_NAME].sh` CLI 명령을 실행하여 웹 인터페이스를 통해 업데이트를 수행하는 대신 Firepower Management Center를 업데이트합니다. (CSCux89875)

지원이 필요한 경우

Firepower System을 선택해 주셔서 감사합니다.

설명서 받기, 시스코 BST(Bug Search Tool) 사용, 서비스 요청 제출 및 Firepower System에 관한 추가 정보 수집에 대한 자세한 내용은 http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html에서 *Cisco 제품 설명서의 새로운 사항*을 참고하십시오.

*Cisco 제품 설명서의 새로운 사항*을 구독하십시오. 여기에서는 모든 새로운 Cisco 기술 및 개정된 시스코 기술 문서가 RSS 피드 형식으로 나와 있으며, 리더 애플리케이션을 사용하여 콘텐츠를 사용자 데스크탑으로 바로 전달합니다. RSS 피드는 무료로 제공되는 서비스입니다.

Firepower System에 대해 문의사항이 있거나 지원이 필요한 경우 시스코 지원에 문의하십시오.

- 시스코지원 사이트 방문: http://support.cisco.com/
- 고객 지원에 시스코이메일 보내기: tac@cisco.com
- 시스코 고객 지원에 전화로 문의(1.408.526.7209 또는 1.800.553.2447)