K13325942: 어플라이언스 모드 iControl REST 취약성 CVE-2022-41800

보안 권고

최초 발행일 : **업데이트 날짜** :

보안 권고 설명

어플라이언스 모드에서 실행할 때 관리자 역할이 할당된 인증된 사용자는 공개되지 않은 `iControl REST` 엔드포인트를 활용하여 어플라이언스 모드 제한을 우회할 수 있습니다. 악용에 성공하면 공격자가 보안 경계를 넘을 수 있습니다. (CVE-2022-41800)

타격

어플라이언스 모드에서 관리자 역할이 할당된 유효한 사용자 자격 증명이 있는 인증된 사용자는 어플라이언스 모드 제한을 우회할 수 있습니다. 이것은 컨트롤 플레인 문제입니다. 데이터 플레인 노출이 없습니다. 어플라이언스 모드는 특정 라이센스에 의해 적용되거나 개별 vCMP(Virtual Clustered Multiprocessing) 게스트 인스턴스에 대해 활성화 또는 비활성화될 수 있습니다.

기기 모드에 대한 자세한 내용은 K12815: 기기 모드 개요를 참조하십시오 .

보안 권고 상태

F5 Product Development는 이 취약점에 ID 1106161 및 1143329(BIG-IP)를 할당했습니다. 이 문제는 CWE-77: 명령에 사용된 특수 요소의 부적절한 무효화('명령 주입') 로 분류되었습니다 .

제품 및 버전이 이 취약점에 대해 평가되었는지 확인하려면 **적용 대상(버전 참조)** 상자를 참조하십시오. 릴리스가 취약한 것으로 알려져 있는지 여부, 취약성의 영향을 받는 구성 요소 또는 기능, 취약성을 해결하는 릴리스, 포인트 릴리스 또는 핫픽스에 대한 정보는 다음 표를 참조하십시오. iHealth 를 사용 하여 BIG-IP 및 BIG-IQ 시스템의 취약성을 진단할 수도 있습니다 . iHealth 사용에 대한 자세한 내용은 K27404821: F5 iHealth를 사용하여 취약성 진단을 참조하십시오 . 보안 권고 버전 관리에 대한 자세한 내용은 K51812227: 보안 권고 버전 관리 이해 를 참조하십시오 .

이 섹션의

- BIG-IP 및 BIG-IQ
- F5OS
- NGINX
- 다른 제품들
- 서비스

BIG-IP 및 BIG-IQ

***참고** : 주어진 부 분기에 대한 수정 사항이 도입된 후 해당 수정 사항은 해당 분기의 모든 후속 유지 관리 및 포인트 릴리스에 적용되며 해당 분기에 대한 추가 수정 사항은 표에 나열되지 않습니다. 예를 들어 수정 사항이 14.1.2.3에 도입되면 수정 사항은 14.1.2.4 및 이후의 모든 14.1.x 릴리스(14.1.3.x., 14.1.4.x)에도 적용됩니다. 자세한 내용은 K51812227: 보안 권고 버전 관리 이해 를 참조하십시오 .*

제품	나뭇가지	취약한 것으로 알려진 버전 [1]	에 도입된 수정 사항	심각성	CVSSv3 점수 [2]	취약한 구성 요소 또는 기능
BIG-IP(모든 모듈)	17.x	17.0.0	없음 [3]	높은	8.7	iControl REST
	16.x	16.1.0 - 16.1.3	없음 [3]			
	15.x	15.1.0 - 15.1.8	없음 [3]			
	14.x	14.1.0 - 14.1.5	없음 [3]			
	13.x	13.1.0 - 13.1.5	없음 [3]			
빅아이피 SPK	모두	없음	해당 없음	취약하지 않음	없음	없음
BIG-IQ 중앙 집중식 관리	모두	없음	해당 없음	취약하지 않음	없음	없음

*[1] F5는 수명 주기의 EoTS(기술 지원 종료) 단계에 아직 도달하지 않은 소프트웨어 버전만 평가합니다. 자세한 내용 은 K4602: F5 보안 취약성 대응 정책 개요의 **보안 핫픽스** 섹션을 참조하십시오 .*

[2] CVSSv3 점수 링크는 AskF5 외부 리소스로 연결되며 문서가 우리 모르게 제거될 수 있습니다.

[3] 이 문제는 지원되는 BIG-IP 버전에 사용할 수 있는 엔지니어링 핫픽스에서 수정되었습니다. 이 문제의 영향을 받는 고객은 F5 지원에서 지원되는 최신 BIG-IP 버전에 대한 핫픽스를 요청할 수 있습니다.

F5OS

제품	나뭇가지	취약한 것으로 알려진 버전 [1]	에 도입된 수정 사항	심각성	CVSSv3 점수 [2]	취약한 구성 요소 또는 기능
F5OS-A	모두	없음	해당 없음	취약하지 않음	없음	없음

F5OS-C	모두	없음	해당 없음	취약하지 않음	없음	없음

*[1] F5는 수명 주기의 EoTS(기술 지원 종료) 단계에 아직 도달하지 않은 소프트웨어 버전만 평가합니다. 자세한 내용 은 K4602: F5 보안 취약성 대응 정책 개요의 **보안 핫픽스** 섹션을 참조하십시오 .*

[2] CVSSv3 점수 링크는 AskF5 외부 리소스로 연결되며 문서가 우리 모르게 제거될 수 있습니다.

NGINX

제품	나뭇가지	취약한 것으로 알려진 버전 [1]	에 도입된 수정 사항	심각성	CVSSv3 점수 [2]	취약한 구성 요소 또는 기능
NGINX(모든 제품)	모두	없음	해당 없음	취약하지 않음	없음	없음

*[1] F5는 수명 주기의 EoTS(기술 지원 종료) 단계에 아직 도달하지 않은 소프트웨어 버전만 평가합니다. 자세한 내용 은 K4602: F5 보안 취약성 대응 정책 개요의 **보안 핫픽스** 섹션을 참조하십시오 .*

[2] CVSSv3 점수 링크는 AskF5 외부 리소스로 연결되며 문서가 우리 모르게 제거될 수 있습니다.

다른 제품들

제품	나뭇가지	취약한 것으로 알려진 버전 [1]	에 도입된 수정 사항	심각성	CVSSv3 점수 [2]	취약한 구성 요소 또는 기능
트래픽스 SDC	모두	없음	해당 없음	취약하지 않음	없음	없음

*[1] F5는 수명 주기의 EoTS(기술 지원 종료) 단계에 아직 도달하지 않은 소프트웨어 버전만 평가합니다. 자세한 내용 은 K4602: F5 보안 취약성 대응 정책 개요의 **보안 핫픽스** 섹션을 참조하십시오 .*

[2] CVSSv3 점수 링크는 AskF5 외부 리소스로 연결되며 문서가 우리 모르게 제거될 수 있습니다.

권장 조치

취약한 것으로 알려진 버전 열에 나열된 버전을 실행 중인 경우 **도입된 수정 사항** 열에 나열된 버전으로 업그레이드하여 이 취약점을 제거할 수 있습니다 . 테이블에 현재 실행 중인 버전보다 이전 버전만 나열되거나 취약하지 않은 버전이 나열되지 않으면 현재 업그레이드 후보가 없는 것입니다.

완화

수정된 버전을 설치할 수 있을 때까지 다음 섹션을 임시 완화로 사용할 수 있습니다. 이러한 완화는 iControl REST에 대한 액세스를 신뢰할 수 있는 네트워크 또는 장치로만 제한하여 공격 표면을 제한합니다. 공격자는 높은 권한을 가진 관리 계정에 대한 유효한 자격 증명을 보유해야 합니다. 따라서 액세스를 제한하면 장치가 여전히 악의적인 내부자 또는 신뢰할 수 있는 범위 내에서 손상된 다른 장치의 측면 이동 위험에 노출될 수 있습니다.

- 자체 IP 주소를 통한 iControl REST 액세스 차단
- 관리 인터페이스를 통한 iControl REST 액세스 차단

자체 IP 주소를 통한 iControl REST 액세스 차단

자체 IP 주소를 통해 BIG-IP 시스템의 iControl REST 인터페이스에 대한 모든 액세스를 차단할 수 있습니다. 이렇게 하려면 시스템의 각 자체 IP 주소에 대해 **포트 잠금** 설정을 **허용 없음 으로 변경할 수 있습니다.** 포트를 열어야 하는 경우 iControl REST에 대한 액세스를 허용하지 않도록 주의하면서 **Allow Custom 옵션을 사용해야 합니다.** 기본적으로 iControl REST는 TCP 포트 443에서 수신합니다. 또는 사용자 정의 포트를 구성할 수 있습니다.

***참고** : 이 작업을 수행하면 자체 IP 주소를 사용하여 구성 유틸리티 및 iControl REST에 대한 모든 액세스가 차단됩니다. 이러한 변경 사항은 고가용성(HA) 구성 중단을 포함하여 다른 서비스에도 영향을 미칠 수 있습니다.*

자체 IP 주소 구성을 변경하기 전에 F5는 다음 문서를 참조할 것을 강력히 권장합니다.

- K17333: 포트 잠금 동작 개요(12.x - 17.x)
- K13092: BIG-IP 시스템에 대한 액세스 보안 개요
- K31003634: Single-NIC BIG-IP Virtual Edition의 구성 유틸리티는 이제 기본적으로 TCP 포트 8443으로 설정됩니다.
- K51358480: 구성을 다시 로드한 후 단일 NIC BIG-IP VE가 기본 관리 httpd 포트로 잘못 되돌아갈 수 있음

자체 IP 주소에 포트 443을 노출해야 하고 특정 IP 범위에 대한 액세스를 제한하려는 경우 BIG-IP 시스템에 내장된 패킷 필터링 기능을 사용할 수 있습니다. 자세한 내용은 다음 문서를 참조하세요.

- K13383: BIG-IP 패킷 필터에 대한 CIDR 네트워크 주소 구성

관리 인터페이스를 통한 iControl REST 액세스 차단

To mitigate this vulnerability for affected F5 products, you should restrict management access to only trusted users and devices over a secure network. For more information about securing access to BIG-IP systems, refer to the following articles:

- K13092: Overview of securing access to the BIG-IP system
- K46122561: Restricting access to the management interface using network firewall rules
- K69354049: Restricting access to the BIG-IP management interface for Configuration utility and iControl REST services using iptables

Acknowledgements

F5 acknowledges Ron Bowes of Rapid7 for bringing this issue to our attention and following the highest standards of coordinated disclosure.

Supplemental Information

- K41942608: Overview of security advisory articles
- K4602: Overview of the F5 security vulnerability response policy
- K4918: Overview of the F5 critical issue hotfix policy
- K8986: F5 product support policies

- K13123: Managing BIG-IP product hotfixes (11.x - 17.x)
- K167: Downloading software and firmware from F5
- K9970: Subscribing to email notifications regarding F5 products
- K9957: Creating a custom RSS feed to view new and updated documents
- K44525501: Overview of BIG-IP data plane and control plane

적용 대상:

Product: BIG-IQ, BIG-IQ Centralized Management
8.2.0, 8.1.0, 8.0.0, 7.1.0

Product: BIG-IP, BIG-IP AFM, BIG-IP Analytics, BIG-IP APM, BIG-IP ASM, BIG-IP DNS, BIG-IP FPS, BIG-IP GTM, BIG-IP Link Controller, BIG-IP LTM, BIG-IP PEM, BIG-IP AAM
17.0.0, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0, 14.1.5, 14.1.4, 14.1.3, 14.1.2, 14.1.0, 13.1.5, 13.1.4, 13.1.3, 13.1.1, 13.1.0

Product: F5OS, F5OS-A, F5OS-C
1.5.0, 1.3.2, 1.3.1, 1.3.0, 1.2.0, 1.1.1, 1.1.0, 1.0.1, 1.0.0

Product: NGINX Products, NGINX Plus, NGINX App Protect WAF, NGINX App Protect DoS, NGINX Unit, NGINX Ingress Controller, NGINX Instance Manager, NGINX Service Mesh, NGINX Controller, NGINX API Connectivity Manager
R27, R26, R25, R24, R23, R22, 3.9.1, 3.9.0, 3.8.0, 3.7.0, 3.6.0, 3.5.0, 3.4.0, 3.3.0, 3.22.5, 3.22.4, 3.22.3, 3.22.2, 3.22.1, 3.22.0, 3.21.0, 3.20.1, 3.20.0, 3.2.0, 3.19.4-APIM, 3.19.3-APIM, 3.19.2-APIM, 3.19.1-APIM, 3.19.0-APIM, 3.18.3, 3.18.2, 3.18.1-APIM, 3.18.1, 3.18.0-APIM, 3.18.0, 3.17.0, 3.16.1, 3.15.0, 3.14.0, 3.13.0, 3.12.1, 3.12.0, 3.11.0, 3.10.0, 3.1.0, 3.0.0, 2.5.1, 2.5.0, 2.4.1, 2.4.0, 2.3.1, 2.3.0, 2.2.2, 2.2.1, 2.2.0, 2.1.2, 2.1.1, 2.1.0, 2.0.3, 2.0.2, 2.0.1, 2.0.0, 1.9.1, 1.9.0, 1.6.0, 1.5.0, 1.4.1, 1.4.0, 1.3.1, 1.3.0, 1.28.0, 1.27.0, 1.26.1, 1.26.0, 1.25.0, 1.24.0, 1.23.0, 1.22.0, 1.21.0, 1.20.0, 1.2.0, 1.12.5, 1.12.4, 1.12.3, 1.12.2, 1.12.1, 1.12.0, 1.11.2, 1.11.1, 1.11.0, 1.10.1, 1.10.0, 1.1.1, 1.1.0, 1.0.4, 1.0.3, 1.0.2, 1.0.1, 1.0.0

Product: 5G Products, BIG-IP SPK
1.6.0, 1.5.0

Product: Traffix SDC
5.2.0, 5.1.0

Product: F5 App Protect, F5 SSL Orchestrator, F5 DDoS Hybrid Defender
17.0.0, 16.1.3, 16.1.1, 16.1.0, 15.1.1, 15.1.0, 14.1.4, 14.1.2, 14.1.0