# K94221585: iControl SOAP 취약점 CVE-2022-41622

## 보안 권고

**최초 발행일** : **업데이트 날짜** :

## 보안 권고 설명

BIG-IP 및 BIG-IQ는 iControl SOAP를 통한 CSRF(Cross-Site Request Forgery) 공격에 취약합니다. ( CVE-2022-41622 )

## 타격

공격자는 최소한 리소스 관리자 역할 권한이 있고 iControl SOAP의 기본 인증을 통해 인증된 사용자를 속여 중요한 작업을 수행하도록 할 수 있습니다. 공격자는 데이터 플레인이 아닌 컨트롤 플레인을 통해서만 이 취약점을 악용할 수 있습니다. 취약점이 악용되면 전체 시스템이 손상될 수 있습니다.

## 보안 권고 상태

F5 Product Development는 이 취약점에 ID 1143073(BIG-IP) 및 1143073-6(BIG-IQ)을 할당했습니다. 이 문제는 CWE-352: CSRF(Cross-Site Request Forgery) 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

### 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 | 8.8 | 아이컨트롤 비누 |
| | 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 | 8.x | 8.0.0 - 8.2.0 | 없음 | 높은 | 8.8 | 아이컨트롤 비누 |
| | 7.x | 7.1.0 | 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] F5는 지원되는 BIG-IP 시스템 버전에 사용할 수 있는 엔지니어링 핫픽스에서 이 문제를 수정했습니다. 이 문제의 영향을 받는 고객은 F5 지원 에서 지원되는 최신 BIG-IP 버전에 대한 핫픽스를 요청할 수 있습니다 . 이 취약점을 해결하려면 이전 표에 나열된 BIG-IP 릴리스 중 하나에 핫픽스를 설치한 후 iControl SOAP에 대한 기본 인증도 비활성화해야 합니다.*

### 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

If you are running a version listed in the **Versions known to be vulnerable** column, you can eliminate this vulnerability by installing a version listed in the **Fixes introduced in** column. If the **Fixes introduced in** column does not list a version for your branch, then no update candidate currently exists for that branch and F5 recommends that you upgrade to a version with the fix (refer to the table).

If the **Fixes introduced in** column lists a version prior to the one you are running, in the same branch, then your version should have the fix.

**BIG-IP**

To eliminate this vulnerability in the BIG-IP system, after installing a version listed in the **Fixes introduced in** column, you must disable Basic Authentication for iControl SOAP. To do so, perform the following procedure:

***Impact of procedure**: Performing the following procedure should not have a negative impact on your system.*

1. Log in to the Traffic Management Shell (**tmsh**) by entering the following command:
   `tmsh`
2. Disable Basic Authentication for iControl SOAP by entering the following command:
   `modify sys db icontrol.basic_auth value disable`
3. Save the configuration by entering the following command:
   `save sys config`

## Mitigation

To mitigate this vulnerability, you can use a unique and isolated web browser when managing the BIG-IP or BIG-IQ system.

This attack cannot be prevented if you have authenticated to iControl SOAP in the web browser with basic authentication. This authentication mechanism is uncommon and is different from using the login page for the Configuration utility. F5 recommends that you do not authenticate with basic authentication in the web browser. If an authentication window for basic authentication pops up on the web browser, do not provide credentials.

If you follow best practices in securing access to the management interface and self IP addresses of BIG-IP and BIG-IQ systems, you help to minimize the attack surface. Review the following articles for guidance:

**For Self IP addresses**

- K13092: Overview of securing access to the BIG-IP system
- K17333: Overview of port lockdown behavior (12.x - 17.x)
- K31003634: The Configuration utility of the Single-NIC BIG-IP Virtual Edition now defaults to TCP port 8443
- K51358480: The single-NIC BIG-IP VE may erroneously revert to the default management httpd port after a configuration reload
- K39403510: Managing the port lockdown configuration on the BIG-IQ system

**For Management interface**

- 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
- K92748202: Restricting access to the BIG-IQ management interface using network firewall rules

***Note**: For BIG-IQ 7.x, secure the management interface by using an external packet filtering device such as the BIG-IP Advanced Firewall Manager (AFM).*

**BIG-IP mitigation**

For the BIG-IP system only, restrict access to the system's iControl SOAP API to only trusted users. If you are not using the iControl SOAP API, then you can disable all access by setting the iControl SOAP API allowed list to an empty list. To do so, perform the following procedure:

1. Log in to tmsh by entering the following command:
   `tmsh`
2. Remove all IP addresses or range of IP addresses from the list of allowed addresses by entering the following command:

3. Save the change by entering the following command:
   ```
   save /sys config
   ```

For more information about limiting access to trusted users, refer to K17459: Restricting access to the iControl SOAP API by source IP address.

**BIG-IQ mitigation**

For the BIG-IQ system only, restrict the iControl SOAP access to localhost (127.0.0.1) by changing the **webd** configuration. To do so, perform the following procedure:

***Impact of procedure**: The BIG-IQ user interface may be momentarily disrupted while the **webd** service restarts.*

1. Log in to the command line of the affected BIG-IQ system as the root user.
2. Back up a copy of the **webd** configuration by entering the following command:
   ```
   cp -p /etc/webd/webd.conf /etc/webd/webd.conf.K94221585
   ```
3. Have a text editor such as **vi** or **nano** available to edit the **webd** configuration.
4. There are two iControl FastCGI endpoint (location **/iControl/iControlPortal.cgi**) configurations; one is under the server configuration stanza listening for port 80, and the other is located under the server configuration stanza listening for port 443 and is enabled with SSL. The one under the port 80 server is already restricted to localhost (127.0.0.1) by default. Restrict the one under the SSL server. The starting of the SSL server configuration stanza should appear similar to the following example:
   ```
   server {
     listen [::]:443 ipv6only=on ssl;
     listen *:443 ssl;
   }
   ```
5. Locate the iControl FastCGI endpoint configuration under this SSL server; it should appear similar to the following example:
   ```
   # iControl FastCGI endpoint
     location /iControl/iControlPortal.cgi {
     access_by_lua_file /usr/lib/webd/lua/icauth.lua;
     fastcgi_pass 127.0.0.1:8202;
     fastcgi_pass_header X-IControl-Session;
     fastcgi_pass_request_body on;
     fastcgi_param QUERY_STRING $query_string;
     fastcgi_param REQUEST_METHOD $request_method;
     fastcgi_param CONTENT_TYPE $content_type;
     fastcgi_param CONTENT_LENGTH $content_length;
     fastcgi_param SCRIPT_NAME '/iControl/iControlPortal.cgi';
   }
   ```
6. Add the following two lines of configuration to this iControl FastCGI endpoint configuration:
   ```
   allow 127.0.0.1;
   deny all;
   ```
7. After you add the two lines of configuration, the iControl FastCGI endpoint configuration should appear similar to the following example:
   ```
   # iControl FastCGI endpoint
     location /iControl/iControlPortal.cgi {
     allow 127.0.0.1;
     deny all;
     access_by_lua_file /usr/lib/webd/lua/icauth.lua;
     fastcgi_pass 127.0.0.1:8202;
     fastcgi_pass_header X-IControl-Session;
     fastcgi_pass_request_body on;
     fastcgi_param QUERY_STRING $query_string;
     fastcgi_param REQUEST_METHOD $request_method;
     fastcgi_param CONTENT_TYPE $content_type;
     fastcgi_param CONTENT_LENGTH $content_length;
     fastcgi_param SCRIPT_NAME '/iControl/iControlPortal.cgi';
   }
   ```
8. Save the changes and exit the text editor.
9. To effect the change, you must restart the **webd** service. To do so, enter the following command:
   ```
   tmsh restart /sys service webd
   ```

## 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
- K9502: BIG-IP hotfix and point release matrix
- K13123: Managing BIG-IP product hotfixes (11.x - 17.x)
- K15106: Managing BIG-IQ product hotfixes
- K15113: BIG-IQ hotfix and point release matrix
- 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