

# SSL Heartbleed 취약성: 영향과 대응책 (part 2)



Jezmynn Koh, 2014-17-04

(1부에서 계속)

그렇다면 클라우드는?

깊은 지식을 가지고 있는 독자라면 클라우드 컴퓨팅은 자신의 독자적인 Heartbleed 위협 프로파일을 가지고 있음을 눈치챈 것이다. 그것은 사실이며, 특정 클라우드의 구축 상황에 따라 위협의 강도가 다르기 때문이다.

전형적인 **LAMP** 클라우드 사이트: 전형적인 클라우드 사이트는 Apache, MySQL 및 PHP가 구동되는 리눅스 배포 (보통 줄여서 LAMP라고 불린다) 인스턴스들을 포함하고 있다. 클라우드가 도입된 것이 상대적으로 최근의 현상이며 Heartbleed 취약성이 2년 전에 알려진 것과 시기가 겹치는 것을 생각할 때, 이런 클라우드 LAMP 사이트들이 가장 위험하다.

**F5 ADC** 하드웨어를 가진 클라우드: 많은 고객들이 자신들의 클라우드 인스턴스들 앞단에 F5의 하드웨어 플랫폼을 두고 있다. F5 ADC가 TCP 연결들을 병합하고, 공통 객체들을 캐시하고, 또한 당연한 일이지만 성능이 많이 요구되는 하드웨어 암호화 연산에 따른 부하를 덜어주기 때문에 효율성이 눈에 띄게 좋아진다. 이런 고객들은 F5가 SSL을 종료하므로 이미 보호되고 있다. 만약 당신이 이런 경우라면, 단순히 가상 서버들이 HTTPS의 암호화를 해제하지 않은 채 내보내지 않도록 하기만 하면 된다. (아래 참조)

**F5 가상 ADC:** 완전히 가상화된 클라우드에서는 F5 모듈도 가상 인스턴스이다. 근본적인 암호화 하드웨어 오프로드가 생기지 않으면, F5 모듈이 HTTPS 서버들을 위해 SSL을 종료하도록 하는 것이 덜 매력적일 것이다. 그러므로 하드웨어로 구축된 앞의 경우에 비해 Heartbleed 위험성이 높아진다. 그러나 이 경우도 F5 플랫폼이 방어를 제공할 수 있는데, 그 이유는 가상 ADC에 내재하는 SSL 스택의 소프트웨어가 Heartbleed에 취약하지 않으며 따라서 충분한 방어를 제공할기 때문이다.

다음 단계

기존 F5 고객들은 단순히 **단일 솔루션**을 읽고 자신이 보유한 F5 디바이스의 안전성을 재확인한 후, 자신이 현재 안전할 뿐 아니라 자신의 애플리케이션들이 지난 2년 동안 Heartbleed에 성공적으로 맞서왔음을 알고 두 다리 뻗고 자면 된다. 만약 도움이 필요할 경우, 아래의 F5에 연락하기를 클릭해서 F5 코리아에 연락을 취하면 된다.

만약 F5가 생소한 고객이라면, F5 코리아에 연락을 취해 현재와 미래의 위협으로부터 자신의 비즈니스를 보호할 것을 권장한다.

[F5에 연락하기](#)

결론

미국의 컴퓨터 공학자인 제럴드 와인버그 (Gerald Weinberg)는 “만약 프로그래머들이 프로그램을 작성하는 것처럼 건축가들이 건물을 짓는다면, 이런 건축물을 찾는 첫 번째 딱따구리가 문명 전체를 파괴해버릴 것이다.”라고 말한 일이 있다.

Heartbleed야말로 바로 그런 딱따구리라고 말할 수 있다.

하지만 좋은 소식은 F5 BIG-IP 디바이스들과 가상 인스턴스들이 벌써 인터넷에 널리 퍼져 있으며 그들이 담당하고 있는 HTTPS 애플리케이션들을 보호하고 있다는 것이다. 운영자들은 그렇게 방어되고 있음을 검증할 수 있으며, 보안 팀과 협력해 자신에 맞는 속도로 시스템을 업그레이드할 수 있다. 그리고 현재 보호받지 못하고 있는 사람들은 단순히 F5에 전화를 걸거나, F5의 시험용 버전을 이용해 보호를 받을 수 있다.

\* 현재 **LTM**에서 **SSL** 터미네이션을 하고 있는 경우, **11.5.0**이나 **11.5.1**에서 디폴트 암호화를 **COMPAT**로 바꿔서 보안 **F5 SSL** 스택을 벗어나게 하지만 않았다면, 보호되고 있다. **F5**의 고객 중 이런 경우는 그 수가 매우 작은 것으로 판명되었다.

만약 **11.5.0** 또는 **11.5.1**을 사용 중이고 관리 인터페이스가 인터넷에 노출되었다면, 취약하다. **BIG-IP** 관리 인터페이스에는 **OpenSSL 1.0.2**이 사용된다. **F5**는 이런 구성을 권장하지 않는다.

**Heartbleed**에 대해 질문이 있으신가요? **F5** 커뮤니티에 물어보세요.

\*F5의 끊임 없이 진화하는 커뮤니티에서 배우세요. 191개 국가의 13만 명이 넘는 뛰어난 사람들로 구성되어 있습니다.

---

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | [f5.com](http://f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)

---

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at [f5.com](http://f5.com). Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113