radware

SSLv3 POODLE Vulnerability

Frequently Asked Questions

Over the last week, the info-security and IT communities exploded about the SSL POODLE vulnerability. We expect that over the course of the next few weeks you will be asked questions by your customers and prospects questions regarding this vulnerability. This document provides more information on the vulnerability and what you can do about it.

What is the SSLv3 POODLE Vulnerability?

On October 15 Google published details of vulnerability in the design of SSL version 3.0. This vulnerability allows the plaintext of secure connections to be calculated by a network attacker. The new vulnerability, named ‘POODLE’, compromises encryption, by forcing a browser or client to use the less secure SSLv3 encryption protocols instead of TLS protocols (eg TLSv1.2). It then carries out a BEAST (Browser Exploit Against SSL/TLS) attack to obtain information from the encrypted stream.

Is This Really Such a Big Issue?

Yes. Although SSL 3.0 is nearly fifteen years old, support for it remains widespread. Most importantly, nearly all browsers support it and, in order to work around bugs in HTTPS servers, browsers will retry failed connections with older protocol versions, including SSL 3.0. Because a network attacker can cause connection failures, they can trigger the use of SSL 3.0 and then exploit this issue.

Are Radware Products Vulnerable?

Radware has tested all of its products and recently announced to customers details about the status of its and mitigation recommendations in regard to CVE-2014-3566. If you are asked, refer your customers to read Radware’s Security Advisory to ensure they are running a non-vulnerable version.

Is There a Solution to Block This Vulnerability?

In its Security Advisory mitigation plan, Radware recommends that SSLv3 is disabled in data interfaces to force clients to work with TLS protocols, while management interfaces (which are less at risk of attack) should use SSH as an option until a full fix is released.

Radware’s team of cyber-security experts is available to our customers 24/7. Contact us if you require immediate support for this vulnerability.

We advise non-Radware customers to seek assistance from their security organization on how to mitigate this vulnerability. We also suggest considering our Attack Mitigation System (AMS) – one of the most sophisticated solutions for protecting against cyber-attacks.

Additional Resources

- Security Advisory – CVE 2014-3566SSLv3 POODLE Vulnerability
- Blog Article – CVE 2014-3566 POODLE: A New Vulnerability