In the implementation of the RSA algorithm in F5 BIG-IP, a vulnerability has been discovered that allows attackers to gain access to encrypted messages.
The problem identified by researchers Hanno Bock, Juraj Somorovsky and Craig Young received CVE-2017-6168. According to her description, “a virtual server configured to use the SSL protocol is vulnerable to the Adaptive Chosen Ciphertext attack (also known as Daniel Bleichenbacher’s attack) on the RSA algorithm, which allows an attacker without access to a private crypto to access encrypted messages and / or attack” man in the middle. “
The vulnerability affects versions of BIG-IP 11.6.0-11.6.2, 12.0.0-12.1.2 HF1, 13.0.0-13.0.0 HF2.
According to representatives of the company F5 Networks, the implementation of this attack is quite complicated.
“In practice, in most cases, an attacker with the ability to intercept traffic can exploit the above vulnerability to access encrypted messages only after the session has ended. This attack works against TLS sessions that use key exchange using the RSA algorithm, “the message says.
According to the head of the cryptographic unit Cloudflare Nick Sullivan (Nick Sullivan), the vulnerability poses a significant danger.
“It’s hard to overestimate how serious this F5 bug is. It’s practically DROWN without SSLv2. If you work with a vulnerable F5 solution, anyone can forge a digital signature with your private RSA key, “Sullivan said.
Recall, in March 2016, it became known about the vulnerability in OpenSSL, which allows a new type of attack on HTTPS – DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability is not specific to OpenSSL and affects the SSLv2 protocol directly. Although the protocol has long been rendered obsolete, it still supports a significant number of servers.
F5 BIG-IP – a line of devices on which you can install various modules from F5 to provide fault tolerance, load balancing, protection, acceleration and optimization of applications, servers and data centers. This is a server platform for a set of software products, which can be characterized by the general term Application Delivery Networking.