CVE	**HTTP/2 DoS attack type**	**Mitigation**
CVE-2019-9512	Ping Flood The attacker sends continual pings to an HTTP/2 peer, causing the peer to build an internal queue of responses. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both, potentially leading to a denial of service.	Configure maximum PING frames received per connection in a minute. If the number of PING frames exceed the configured limit, NetScaler drops packets on the connection. set httpprofile <profile_name> -http2MaxPingFramesPerMin <value>
CVE-2019-9514	Reset Flood The attacker opens a number of streams and sends an invalid request over each stream that should solicit a stream of RST_STREAM frames from the peer. Depending on how the peer queues the RST_STREAM frames, this can consume excess memory, CPU, or both, potentially leading to a denial of service.	Configure maximum RESET frames sent per connection in a minute. If the number of RESET frames exceed the configured limit, NetScaler drops packets on the connection. set httpprofile <profile_name> -http2MaxResetFramesPerMin <value>
CVE-2019-9515	Settings Flood The attacker sends a stream of SETTINGS frames to the peer. Since the RFC requires that the peer reply with one acknowledgement per SETTINGS frame, an empty SETTINGS frame is almost equivalent in behavior to a ping. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both, potentially leading to a denial of service.	Configure maximum SETTINGS frames received per connection in a minute. If the number of SETTINGS frames exceed the configured limit, NetScaler drops packets on the connection. set httpprofile <profile_name> -http2MaxSettingsFramesPerMin <value>
CVE-2019-9518	Empty Frame Flooding The attacker sends a stream of frames with an empty payload and without the end-of-stream flag. These frames can be DATA, HEADERS, CONTINUATION and/or PUSH_PROMISE. The peer spends time processing each	Configure maximum frames with empty payload, received per connection in a minute. If the number of empty frames exceed the configured limit, NetScaler drops packets on the connection. set httpprofile <profile_name>

	frame disproportionate to attack bandwidth. This can consume excess CPU, potentially leading to a denial of service.	-http2MaxEmptyFramesPerMin <value>
CVE-2023-44487	Rapid Reset Attack The attacker opens several HTTP/2 streams on an HTTP/2 connection and immediately cancels these streams by sending RESET STREAM frames. NetScaler consumes excess memory, CPU, or both, potentially leading to a denial of service.	Configure maximum RESET frames received per connection in a minute. If the number of RESET frames exceed the configured limit, NetScaler drops packets on the connection. set httpprofile <profile_name> -http2MaxRxResetFramesPerMin <value>