OFFZONE 2026

I’ll hack you via a SYN packet

Maxim Suhanov

CICADA8

CVE-2026-10817

NetScaler ADC

Load Balancer

Generic TCP

HTTP(S)

Database connections

GSLB: across data centers

Content Switching

One site, many backends

WAF

Web app protection

Clusters & HA pairs

Cluster: many NetScalers

HA: one active, one standby

And more...

Anti-Bot

Anti-DDoS

TCP flow optimization

And even more!

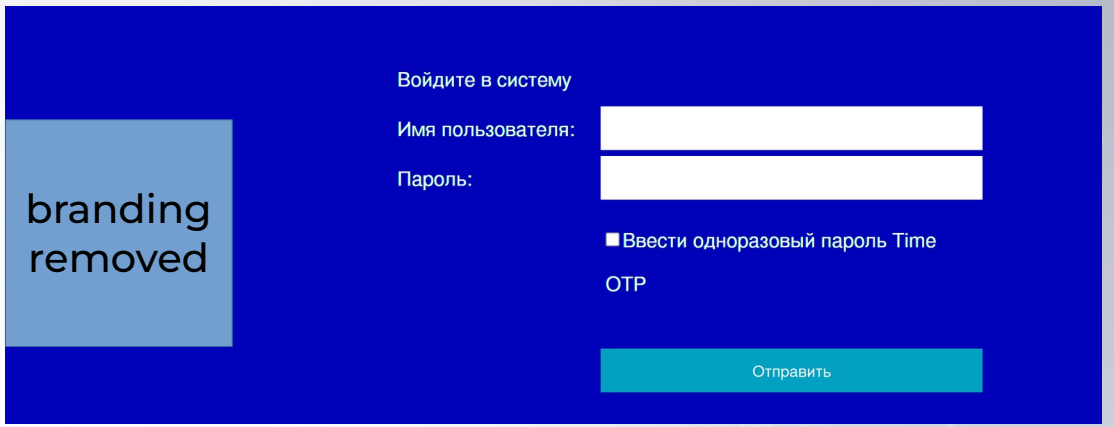
Gateway

NetScaler Gateway

Citrix VDI

Remote desktop (VDI)

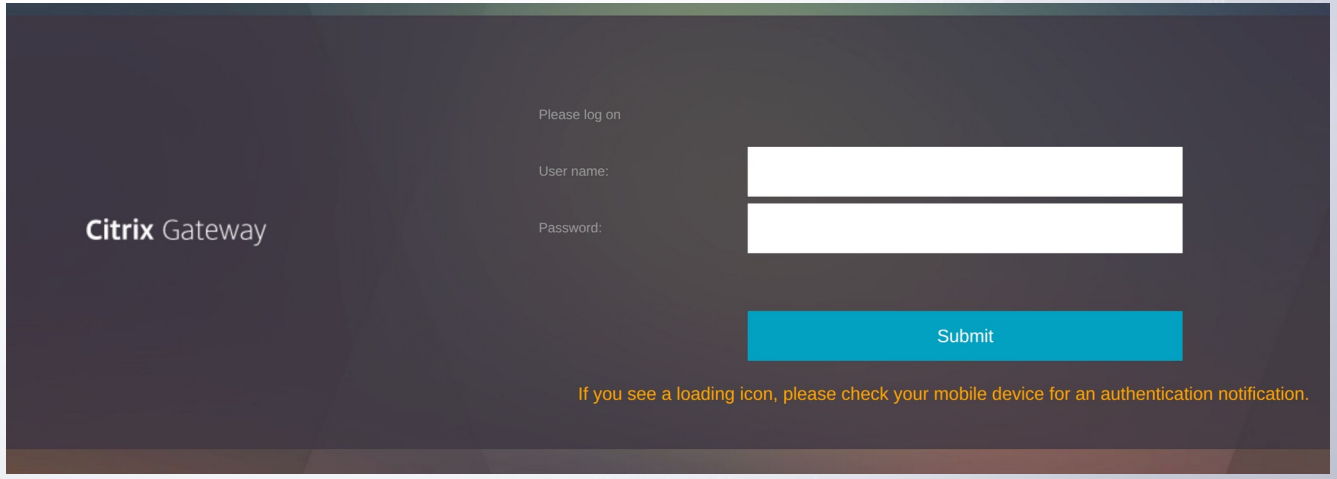
Remote apps



VPN and more

VPN

Clientless VPN (browser-based)



Under the hood

FreeBSD 11.4

VPX (VM) and MPX (HW)

No ASLR

/netscaler/nsppe

≈ 40 MB of compiled C code (with stack cookies)

3 of 12

CISA KEV hits exploited in ransomware campaigns

Bugs from the 90’s

Are here!

TCP Timestamps

- Designed to protect against wrapped TCP sequence numbers
- Can be used to measure RTT
- Old operating systems used “ticks since boot”

  → People disable TCP Timestamps for compliance! 🤡

Internet Engineering Task Force (IETF) — D. Borman, Quantum Corporation
Request for Comments: 7323 — B. Braden, University of Southern California
Obsoletes: 1323 — V. Jacobson, Google, Inc.
Category: Standards Track — R. Scheffenegger, Ed., NetApp, Inc.
ISSN: 2070-1721 — September 2014

TCP Extensions for High Performance

TCP Timestamps in NetScaler

- Disabled by default
- To enable (in TCP profile):

  SYN Cookies → **OFF**

  TCP Timestamps → **ON**

TCP Timestamps

SYN:

```
Transmission Control Protocol, Src Port: 37992, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 37992
    Destination Port: 443
    [Stream index: 2]
    [Stream Packet Number: 1]
  ▸ [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4001998947
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x869a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window
    ▸ TCP Option - Maximum segment size: 1460 bytes
    ▸ TCP Option - SACK permitted
    ▾ TCP Option - Timestamps: TSval 483628492, TSecr 0
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 483628492
        Timestamp echo reply: 0
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Window scale: 10 (multiply by 1024)
```

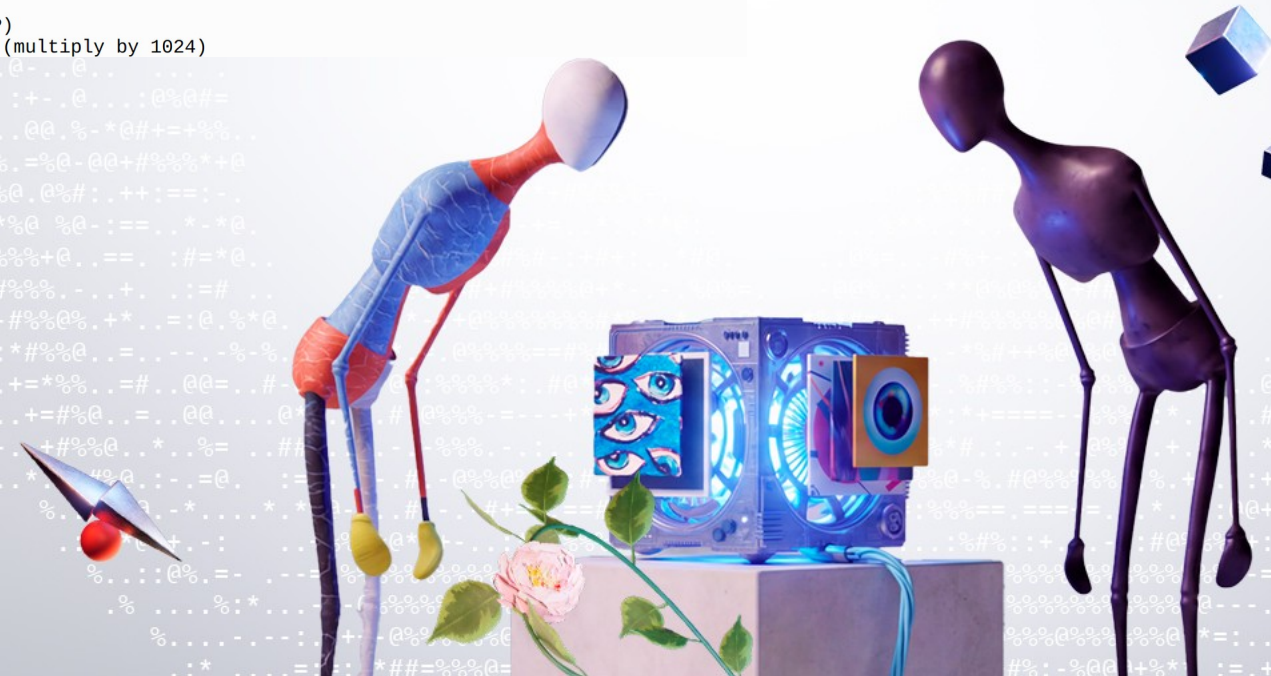
SYN+ACK:

```
Transmission Control Protocol, Src Port: 443, Dst Port: 37992, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 37992
    [Stream index: 2]
    [Stream Packet Number: 2]
  ▸ [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 9528025
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4001998948
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xe14f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Windo
    ▸ TCP Option - Maximum segment size: 1420 bytes
    ▸ TCP Option - SACK permitted
    ▾ TCP Option - Timestamps: TSval 875391250, TSecr 483628492
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 875391250
        Timestamp echo reply: 483628492
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Window scale: 8 (multiply by 256)
```

What if...

```
▾ Transmission Control Protocol, Src Port: 37992, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 37992
    Destination Port: 443
    [Stream index: 2]
    [Stream Packet Number: 1]
  ▸ [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4001998947
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x869a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window
    ▸ TCP Option - Maximum segment size: 1460 bytes
    ▸ TCP Option - SACK permitted
    ▾ TCP Option - Timestamps: TSval 483628492, TSecr 0
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 483628492
        Timestamp echo reply: 0
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - Window scale: 10 (multiply by 1024)
```

... I cut the packet here?



What if...

SYN (perfectly routable):

```
Transmission Control Protocol, Src Port: 52395, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 52395
    Destination Port: 443
    [Stream index: 6]
    [Stream Packet Number: 1]
  ▸ [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 511903529
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0110 .... = Header Length: 24 bytes (6)
  ▸ Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x8005 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (4 bytes), No-Operation (NOP), No-Operation (NOP)
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - No-Operation (NOP)
    ▾ Timestamps (option length = 10 bytes says option goes past end of options)
      ▾ [Expert Info (Note/Sequence): Timestamps (option length = 10 bytes says option goes past en…
          [Timestamps (option length = 10 bytes says option goes past end of options)]
          [Severity level: Note]
          [Group: Sequence]
  ▸ [Timestamps]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
```

SYN+ACK:

```
Transmission Control Protocol, Src Port: 443, Dst Port: 52395, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 52395
    [Stream index: 6]
    [Stream Packet Number: 2]
  ▸ [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2492461908
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 511903530
    1001 .... = Header Length: 36 bytes (9)
  ▸ Flags: 0x012 (SYN, ACK)
    Window: 8190
    [Calculated window size: 8190]
    Checksum: 0x1560 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (16 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), Timestamps
    ▸ TCP Option - Maximum segment size: 536 bytes
    ▸ TCP Option - No-Operation (NOP)
    ▸ TCP Option - No-Operation (NOP)
    ▾ TCP Option - Timestamps: TSval 3045873775, TSecr 3796934204
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 3045873775
        Timestamp echo reply: 3796934204
    ▾ [Expert Info (Note/Protocol): The SYN packet does not contain a SACK PERM option]
        [The SYN packet does not contain a SACK PERM option]
        [Severity level: Note]
        [Group: Protocol]
```

Bytes from the OOB read

Just 4 bytes!

- Come from the preallocated packet buffer
  - ✓ One buffer per receive queue
- Allocation length is much larger than MTU
  - ✓ Even with Jumbo frames
- Leaks can be chained
  - ✓ 8, 12, or more adjacent bytes via 2, 3, or more SYNs
  - ✓ Just add NOPs before the Timestamp option
  - ✓ Need high transfer rate

Is it dangerous?

- We live in the HTTPS era
- But HTTPS can be decrypted before NetScaler
- Also, IPsec gets decrypted in-place

```
--2026-04-02 15:32:58--  http://10.128.0.100/afaf
Connecting to 10.128.0.100:80... connected.
HTTP request sent, awaiting response... Read error (Connection timed
Giving up.

--2026-04-02 15:32:58--  http://10.128.0.100/afaf
Connecting to 10.128.0.100:80... connected.
HTTP request sent, awaiting response... Read error (Connection timed
Giving up.

--2026-04-02 15:32:59--  http://10.128.0.100/afaf
Connecting to 10.128.0.100:80... connected.
HTTP request sent, awaiting response... Read error (Connection timed
Giving up.

--2026-04-02 15:32:59--  http://10.128.0.100/afaf
Connecting to 10.128.0.100:80... connected.
HTTP request sent, awaiting response... Read error (Connection timed
Giving up.

--2026-04-02 15:32:59--  http://10.128.0.100/afaf
Connecting to 10.128.0.100:80... connected.
HTTP request sent, awaiting response... Read error (Connection timed
Giving up.

--2026-04-02 15:32:59--  http://10.128.0.100/afaf
Connecting to 10.128.0.100:80... connected.
HTTP request sent, awaiting response... Read error (Connection timed
Giving up.
```

```
==================================================================
ANALYSIS of 10124 leaked 4-byte values (40496 bytes total)
==================================================================

  Unique values : 2781 / 10124  (27.5%)
  Zero values   : 581 / 10124  (5.7%)
  Non-zero      : 9543 / 10124  (94.3%)

  Top 20 most common values:
    0x0101080A  (....)  ×4293
    0x66204854  (f HT)  ×756
    0x00000000  (....)  ×581
    0xBEBAADDE  (....)  ×175
    0x47455420  (GET )  ×48
    0x01010402  (....)  ×45
    0x2F616661  (/afa)  ×39
    0xF9B267F8  (..g.)  ×21
    0xF9B26DBE  (..m.)  ×20
    0xF9B2523F  (..R?)  ×20
    0xF9B276CE  (..v.)  ×19
    0xF9B27FDE  (....)  ×19
    0xF9B26935  (..i5)  ×17
    0xF9B288EE  (....)  ×17
    0x00000004  (....)  ×17
    0x09090901  (....)  ×16
    0xF9B254B3  (..T.)  ×15
    0xF9B27454  (..tT)  ×15
    0xF9B26B45  (..kE)  ×14
    0xF9B27172  (..qr)  ×14
```

/0 scan results

- > 130 vulnerable hosts (NetScaler VIPs) leaking *at least something*

- Only one port was scanned (443/TCP)
- Leaked data discarded; this was a “no crash” scan
- Don’t go beyond the vulnerability check
- Report the vulnerability to all who provide a security contact
  - ✓ After the fix is available

- Zero complaints received via the exclusion form
- Zero complaints received via ISP

Disclosure timeline

- 2026-04-06 vulnerability reported
- 2026-04-10 vendor reproduced and escalated internally

  [...]
- 2026-06-30 fix released

CVSS v4.0 Base Score: 6.9

vs.

CVSS 3.x Severity and Vector Strings:

NVD **NIST:** NVD **Base Score:** 7.5 HIGH

OFFZONE
2026

Thank you!
Questions?

OFFZONE 2026

MS

@ERRNO_FAIL

Blog: dfir.ru