teradici®

Security Advisory

- **Advisory ID:** TERA-SA-000056
  CVE Numbers and Scores:
  - CVE-2020-11901
    - Base Score: 9.0
  - CVE-2020-11900
    - Base Score: 8.2
  - CVE-2020-11898
    - Base Score: 7.5
  - CVE-2020-11896
    - Base Score: 7.5
  - CVE-2020-11902
    - Base Score: 7.3
  - CVE-2020-11904
    - Base Score: 5.6
  - CVE-2020-11905
    - Base Score: 5.3
  - CVE-2020-11906
    - Base Score: 5.0
  - CVE-2020-11907
    - Base Score: 5.0
  - CVE-2020-11911
    - Base Score: 3.7
  - CVE-2020-11913
    - Base Score: 3.7
  - CVE-2020-11912
    - Base Score: 3.7
  - CVE-2020-11910
    - Base Score: 3.7
  - CVE-2020-11909
    - Base Score: 3.7
  - CVE-2020-11914
    - Base Score: 3.1
- **Published:** 17 June 2020
- **Last Updated:** 17 June 2020

Summary

Multiple vulnerabilities have been discovered in the Treck IP stack used in the Tera2 Zero Client and Remote Workstation Card firmware.

Affected Products

- Tera2 Zero Client firmware 20.01.1 and earlier
- Tera2 Remote Workstation Card 20.01.1 and earlier

Solutions and Mitigations

Available Updates

Teradici released **Zero Client firmware** versions 17.05.0, 20.01.3, and 20.04.1 to address these vulnerabilities.

Teradici released **Remote Workstation Card** versions 17.05.0, 20.01.3, and 20.04.1 to address these vulnerabilities.

Workarounds and Mitigation

There are no workarounds that address this vulnerability. To mitigate the vulnerabilities, update to one of the versions of **Zero Client firmware** or **Remote Workstation Card** listed above, **(or later).**

Vulnerability Details

CVE-2020-11901

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 9.0

CVE-2020-11900

View the full description on the MITRE website.

- Problem Type:
  - Possible Double Free (CWE-415)

  CVSS Vector String: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
  - Base Score: 8.2

CVE-2020-11898

View the full description on the MITRE website.

Please note that the base score of this CVE publication has been modified reflect the severity of the vulnerability when used in Teradici products.

- Problem Type:
  - Improper Handling of Length Parameter (CWE-130)

  CVSS Vector String: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5

CVE-2020-11896

View the full description on the MITRE website.

Please note that the base score of this CVE publication has been modified reflect the severity of the vulnerability when used in Teradici products.

- Problem Type:
  - Improper Handling of Length Parameter (CWE-130)

  CVSS Vector String: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5

CVE-2020-11902

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
  - Base Score: 7.3

CVE-2020-11904

View the full description on the MITRE website.

- Problem Type:
  - Possible Integer Overflow or Wraparound (CWE-190)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
  - Base Score: 5.6

CVE-2020-11905

View the full description on the MITRE website.

- Problem Type:
  - Possible Out-of-bounds Read (CWE-125)

  CVSS Vector String: AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.3

CVE-2020-11906

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
  - Base Score: 5.0

CVE-2020-11907

View the full description on the MITRE website.

- Problem Type:
  - Improper Handling of Length Parameter (CWE-130)

  CVSS Vector String: AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
  - Base Score: 5.0

CVE-2020-11911

View the full description on the MITRE website.

- Problem Type:
  - Improper Access Control (CWE-284)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
  - Base Score: 3.7

CVE-2020-11913

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 3.7

CVE-2020-11912

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 3.7

CVE-2020-11910

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 3.7

CVE-2020-11909

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 3.7

CVE-2020-11914

View the full description on the MITRE website.

- Problem Type:
  - Improper Input Validation (CWE-20)

  CVSS Vector String: AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
  - Base Score: 3.1

Remark

Vulnerability classification has been performed using the CVSSv3 scoring system. The CVSS environmental score is specific to each customerâ€™s environment and should be defined by the customer to attain a final scoring.

Additional Resources

- [1] Zero Client firmware 17.05.0
- [2] Zero Client firmware 20.01.3
- [3] Zero Client firmware 20.04.1
- [4] Remote Workstation Card 17.05.0
- [5] Remote Workstation Card 20.01.3
- [6] Remote Workstation Card 20.04.1

Revision History

17 June 2020: Initial Publication