Security Advisory 2021-027

Multiple Vulnerabilities in Citrix

June 10, 2021 — v1.0

TLP:WHITE

History:

- *10/06/2021 — v1.0 – Initial publication*

Summary

On the 8th of June, Citrix released a Security Update about CVE-2020-8299 (medium severity) and CVE-2020-8300 (high severity) vulnerabilities [1]. The medium severity vulnerability is a network-based denial-of-service. The high severity vulnerability is a SAML authentication hijacking caused by an improper access control [2].

Technical Details

CVE-2020-8299 is a network-based denial-of-service vulnerability. The attacker must be in the same Layer 2 network segment as the vulnerable appliance and the affected products are Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP.

CVE-2020-8300 is a SAML authentication hijack vulnerability caused by an improper access control. By using a phishing attack, the exploitation of this vulnerability may allow an attacker to steal a valid user session. The affected products are Citrix ADC or Citrix Gateway which must be configured as a SAML SP or a SAML IdP.

There are no additional technical details shared by Citrix.

Products Affected

CVE-2020-8299 affects the following supported versions of Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP:

- Citrix ADC and Citrix Gateway 13.0 before 13.0-76.29
- Citrix ADC and Citrix Gateway 12.1 before 12.1-61.18
- Citrix ADC and NetScaler Gateway 11.1 before 65.20
- Citrix ADC 12.1-FIPS before 12.1-55.238
- Citrix SD-WAN WANOP 11.4 before 11.4.0
- Citrix SD-WAN WANOP 11.3 before 11.3.2
- Citrix SD-WAN WANOP 11.3 before 11.3.1a
- Citrix SD-WAN WANOP 11.2 before 11.2.3a
- Citrix SD-WAN WANOP 11.1 before 11.1.2c
- Citrix SD-WAN WANOP 10.2 before 10.2.9a

CVE-2020-8300 is applied to the following supported versions of Citrix ADC and Citrix Gateway:

- Citrix ADC and Citrix Gateway 13.0. before 13.0-82.41
- Citrix ADC and Citrix Gateway 12.1 before 12.1-62.23
- Citrix ADC and NetScaler Gateway 11.1 before 11.1-65.20
- Citrix ADC 12.1-FIPS before 12.1-55.238

These issues have already been addressed in Citrix-managed cloud services such as Citrix Gateway Service and Citrix Secure Workspace Access. Customers using Citrix-managed services do not need to take any additional action.

Recommendations

Citrix recommends the affected customers to install relevant updates as soon as possible.

For CVE-2020-8300, when the Citrix ADC and/or Citrix Cloud Gateway are used as a SAML SP, SAML IdP, or both, upgrade to at least the following versions:

- Citrix ADC and Citrix Gateway 13.0-82.41
- Citrix ADC and NetScaler Gateway ADC 12.1-62.23
- Citrix ADC and NetScaler Gateway 11.1-65.20
- Citrix ADC 12.1-FIPS 12.1-55.238

For CVE-2020-8299, the Citrix ADC, Citrix Gateway, and Citrix SD-WAN WANOP should be upgraded to at least the following versions:

- Citrix ADC and Citrix Gateway 13.0-76.29
- Citrix ADC and Citrix Gateway 12.1-61.18
- Citrix ADC and NetScaler Gateway 11.1-65.20
- Citrix ADC 12.1-FIPS 12.1-55.238
- Citrix SD-WAN WANOP 11.4.0
- Citrix SD-WAN WANOP 11.3.2
- Citrix SD-WAN WANOP 11.3.1a
- Citrix SD-WAN WANOP 11.2.3a
- Citrix SD-WAN WANOP 11.1.2c
- Citrix SD-WAN WANOP 10.2.9a

References

[1] https://support.citrix.com/article/CTX297155

[2] https://dirteam.com/sander/2021/06/08/saml-authentication-hijack-vulnerability-on-citrix-adc-and-citrix-gateway-appliances-cve-2020-8300/