



NCSC-2024-0288

Kwetsbaarheden verholpen in Citrix Workspace, NetScaler ADC en NetScaler Gateway

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-07-2024

Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

De volgende CVE's zijn toegevoegd: * CVE-2024-6286 * CVE-2024-2636 * CVE-2024-6151 * CVE-2024-6150 * CVE-2024-6748

Feiten

Citrix heeft een aantal kwetsbaarheden verholpen in Workspace, NetScaler ADC en NetScaler Gateway

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Verhoogde gebruikersrechten

Oplossingen

Citrix heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Voor meer informatie, zie bijgevoegde referenties.

Referenties

- <https://api.first.org/data/v1/epss?cve=CVE-2024-5491>
- <https://api.first.org/data/v1/epss?cve=CVE-2024-5492>
- <https://api.first.org/data/v1/epss?cve=CVE-2024-6148>
- <https://api.first.org/data/v1/epss?cve=CVE-2024-6150>
- <https://api.first.org/data/v1/epss?cve=CVE-2024-6151>
- <https://api.first.org/data/v1/epss?cve=CVE-2024-6236>
- <https://api.first.org/data/v1/epss?cve=CVE-2024-6286>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-5491>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-5492>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-6148>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-6150>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-6151>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-6236>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-6286>
- <https://wid.cert-bund.de/well-known/csaf/white/2024/wid-sec-w-2024-1557.json>

- <https://wid.cert-bund.de/.well-known/csaf/white/2024/wid-sec-w-2024-1558.json>
- <https://wid.cert-bund.de/.well-known/csaf/white/2024/wid-sec-w-2024-1559.json>
- <https://wid.cert-bund.de/.well-known/csaf/white/2024/wid-sec-w-2024-1561.json>
- <https://wid.cert-bund.de/.well-known/csaf/white/2024/wid-sec-w-2024-1577.json>
- <https://www.cve.org/CVERecord?id=CVE-2024-5491>
- <https://www.cve.org/CVERecord?id=CVE-2024-5492>
- <https://www.cve.org/CVERecord?id=CVE-2024-6148>
- <https://www.cve.org/CVERecord?id=CVE-2024-6150>
- <https://www.cve.org/CVERecord?id=CVE-2024-6151>
- <https://www.cve.org/CVERecord?id=CVE-2024-6236>
- <https://www.cve.org/CVERecord?id=CVE-2024-6286>
- <https://support.citrix.com/article/CTX677944/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20245491-and-cve20245492>
- <https://support.citrix.com/article/CTX677998/netscaler-console-agent-and-svm-security-bulletin-for-cve20246235-and-cve20246236>
- <https://support.citrix.com/article/CTX678035/windows-virtual-delivery-agent-for-cvad-and-citrix-daas-security-bulletin-cve20246151>
- <https://support.citrix.com/article/CTX678036/citrix-workspace-app-for-windows-security-bulletin-cve20246286>
- <https://support.citrix.com/article/CTX678037/citrix-workspace-app-for-html5-security-bulletin-cve20246148-and-cve20246149>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-5492	
➤ CVE-2024-5491	
➤ CVE-2024-6286	
➤ CVE-2024-6236	
➤ CVE-2024-6151	
➤ CVE-2024-6150	
➤ CVE-2024-6148	

CWE's

CWE	Beschrijving
> CWE-404	Improper Resource Shutdown or Release
> CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

Getroffen producten

netsclaer
netscaler_console
netscaler_adc
citrix
netscaler_application_delivery_controller
netscaler_gateway
netscaler_gateway_firmware
application_delivery_management
citrix_provisioning
citrix_workspace_app_for_html5
citrix_workspace_app_for_windows
netscaler_agent
netscaler_console
netscaler_svm
provisioning_services
virtual_apps_and_desktops
windows_virtual_delivery_agent
workspace_app
workspace

netScaler
agent
netScaler_adc
netScaler_gateway
sdx

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.