URGENT: Kwetsbaarheid in Citrix ADC & Citrix Gateway Servers, impactinschatting “Zeer Hoog”

2020-01-14 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET vraagt dringend aandacht voor onderstaand bericht met betrekking tot de kwetsbaarheid in Citrix ADC & Citrix Gateway Servers, waarvan de eventuele impact wordt ingeschat op “Zeer Hoog”.

https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen

Deze kwetsbaarheid dient als een zero-day behandeld te worden binnen uw organisatie, waar op dit moment nog geen patch voor beschikbaar is. Organisaties die nog niet, of relatief laat de mitigerende maatregelen hebben toegepast zijn zeer waarschijnlijk gecompromitteerd. Het Cyber Defense Center van ESET Nederland biedt daarom aan om uw organisatie te ondersteunen bij het vaststellen van de impact voor uw omgeving. Wilt u onze hulp inschakelen? Neem dan contact op via de volgende stappen:

1. Stuur een mail naar securityservices@eset.nl met onderwerp: Citrix Onderzoek
2. Stuur ons de contactgegevens van de persoon waar direct contact mee opgenomen kan worden omtrent het onderzoek
3. Onze Security Engineers nemen zo spoedig mogelijk contact op

Wenst u snel contact, of heeft u vermoeden van een incident, neem dan direct contact op met Maria Gil-Palacios via maria.gilpalacios@eset.nl of +31 (0)6 11478765.

Indien de mitigerende maatregelen nog niet zijn genomen adviseert ESET het volgende:

1. Implementeer meteen de mitigerende maatregelen
2. Stel de logging veilig
3. Onderzoek de systemen op sporen van onrechtmatige toegang

Zie voor meer informatie ook de volgende URL:
https://www.reddit.com/r/blueteamsec/comments/en4m7j/multiple_exploits_for_cve201919781_citrix/

Let op: Aanvallers zouden reeds succesvol gegevens kunnen hebben verkregen die later gebruikt zouden kunnen worden in een aanval. Wanneer uw Citrix Netscaler-omgeving nog niet is beschermd door middel van tweefactorauthenticatie, dan kunt u hier per direct een triallicentie voor aanvragen om deze op korte termijn eenvoudig te voorzien van een extra beveiligingslaag. Zie ook de volgende URL:
https://techcenter.eset.nl/kb/articles/how-do-i-configure-my-citrix-netscaler-device-for-use-with-eset-secure-authentication