



Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid

NCSC | Beveiligingsadviezen

- [Home](#)
- [Beveiligingsadviezen](#)
- [NCSC-2020-0367](#)

Beveiligingsadviezen

Beveiligingsadvies; NCSC-2020-0367

[▶ Download](#)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

```
#####  
##  N C S C ~ B E V E I L I G I N G S A D V I E S  ##  
#####
```

Titel : Kwetsbaarheid ontdekt in HiveOS
Advisory ID : NCSC-2020-0367
Versie : 1.00
Kans : high
CVE ID :
(Details over de kwetsbaarheden kunt u vinden op de Mitre website: <http://cve.mitre.org/cve/>)
Schade : medium
Denial-of-Service (DoS)
Uitgiftedatum : 20200507
Toepassing : Aerohive AP
Versie(s) : <=11.x
Platform(s) :

Beschrijving

Er is een kwetsbaarheid ontdekt in HiveOS. Een niet geauthenticeerde kwaadwillende op afstand kan de kwetsbaarheid mogelijk misbruiken om een Denial-of-Service (DoS) te veroorzaken. Hierdoor wordt de applicatie tijdelijk onbereikbaar. De kwaadwillende dient hiervoor een geprepareerd HTTP request te versturen naar de web server van de hive user interface.

Er is PoC code verschenen. Er is (nog) geen beveiligingskenmerk aan deze kwetsbaarheid toegewezen.

Mogelijke oplossingen

Extreme Networks heeft nog geen updates beschikbaar gesteld voor het verhelpen van de kwetsbaarheid. Volgens de onderzoekers wordt de applicatie 5 minuten onbereikbaar na uit uitvoeren van de PoC code. Wij adviseren de beschikbaarheid van de HiveOS oplossingen te monitoren om mogelijk misbruik van de kwetsbaarheid te detecteren.

Vrijwaringsverklaring

Door gebruik van deze security advisory gaat u akkoord met de navolgende voorwaarden. Ondanks dat het NCSC de grootst mogelijke zorg heeft betracht bij de samenstelling van dit beveiligingsadvies, kan het NCSC niet instaan voor de volledigheid, juistheid of (voortdurende) actualiteit van dit beveiligingsadvies. De informatie in dit beveiligingsadvies is uitsluitend bedoeld als algemene informatie voor professionele partijen. Aan de informatie in dit beveiligingsadvies kunnen geen rechten worden ontleend. Het NCSC en de Staat zijn niet aansprakelijk voor enige schade ten gevolge van het gebruik of de onmogelijkheid van het gebruik van dit beveiligingsadvies, waaronder begrepen schade ten gevolge van de onjuistheid of onvolledigheid van de informatie in dit beveiligingsadvies. Op dit beveiligingsadvies is Nederlands recht van toepassing. Alle geschillen in verband met en/of voortvloeiend uit dit beveiligingsadvies zullen worden voorgelegd aan de exclusief bevoegde rechter te Den Haag. Deze rechtskeuze geldt tevens voor de voorzieningenrechter in kort geding.

-----BEGIN PGP SIGNATURE-----

Version: Encryption Desktop 10.4.2 (Build 502)

Charset: utf-8

wsDVAwUBXrQGQk/4qUtG/lqjAQreNgwAph9w0TivAZqRfbreIx2Sl0IT7nWmA51A
2j0UfN/xEINGLBYTFg+w4ywEV/ThxsUmSvZKohZ2sVj4P2ArgauxGWHM3Cs6H2wf
j+JxaawJgWDAbFWwdy+TBq6Rez/VtEo6c9nmUxtAYDei8Z/AFtNMK51kRLIw5yqr
P9DYnjDF8dKKZmTswXJ0LYQwy7gc6l4aX6sUPoQecAJo+xepjJGv+tTjJG02Aj6Y
DU8B7esJ5awXo8bWDriDeHnbiUjrP0Zai790a7HnncxvuLF0qTQCFmsZzWegNl+S
wzLB7plDVpC+cRlnU8rSfgivnyMZTFCN6RF8SPMceMtbCYIqpJJimSFjTu0kyXjl
KyW/QgyMyIU8pD8zPWAfSviQLxVjGCaPIq/zGV9Nqog+HxYWWcl9AbGU0rddCsBT
K3xV5YMJmBN3Ni0XKowNt/ac/ZKYcRtQNrnLjHn+5e+PikM0iEhgQKFiKNSeXA7x
/XR2sFrn1HA6r0fBZez3cE6tN8C+fFvc

=xUSV

-----END PGP SIGNATURE-----