**TLP:WHITE**
**Szabadon terjeszthető!**

# Rendkívüli tájékoztató

## Nagios és Nagios XI termékek érintő sérülékenységgel kapcsolatban

(2021.július 09.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztatót** ad ki **Nagios és Nagios XI** termékek **sérülékenységével** kapcsolatban.

2021.06.03-án publikálásra került a Githubon[1] egy Nagios és Nagios XI termékeket érintő sérülékenység, amely lehetővé teszi, hogy egy már **autentikált** támadó távolról **tetszőleges kódokat futtasson** ezeken a termékeken, illetve akár **ellátási lánc elleni támadás** (lásd: SolarWinds[2] incidens) is kivitelezhető ezekkel összefüggésben.

A Nagios termékek lehetővé teszik a felhasználóknak a szoftver funkcionalitásának módosítását ún. dashleteken keresztül, azonban ─ mint az bizonyításra került ─ ez bármiféle **kódellenőrzés nélkül** valósul meg. Ezt a biztonsági hiányosságot egy támadó kihasználhatja például egy **speciális szerkesztett** dashlettel, amelyben káros kódot helyez el, vagy egy **fejlesztői fiók kompromittálódásával**, amelynek segítségével a dashletekbe még azok **kiadása előtt** rejthet káros komponenseket.

**Egy káros dashlet jelentős biztonsági problémát okozhat, ezért a következő lépések javasoltak, hogy megvédjük a hálózatunkat:**

- Mindig ellenőrizzük a dashletek forrásait telepítésük előtt! Kizárólag olyan dashleteket telepítsünk, amelyek jól ismert forrásból származnak!
- További biztonsági intézkedésként javasolt kategorizálás és forgalomszűrés fehérlistázás segítségével, amelyek csökkentik egy ellátási lánc elleni támadás, vagy távoli kódfuttatás végrehajtásának lehetőségét.
- Mindig ellenőrizzük a külső kódokat telepítés előtt.

**Az NBSZ NKI jelenleg nem rendelkezik arra vonatkozó információval, hogy ez a sérülékenység aktív kihasználás alatt állna.**

**Nemzetbiztonsági Szakszolgálat**
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu

[1] https://github.com/ArianeBlow/NagiosXI-EmersonFI

[2] https://nki.gov.hu/it-biztonsag/hirek/az-utobbi-evek-legnagyobb-volumenu-kiberkemkedesi-muveletere-derult-feny/