

TLP: WHITE

Szabadon terjeszthető!

Rendkívüli tájékoztató

Apache HTTP Server 0. napi sérülékenységgel kapcsolatban

(2021. október 08.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztatót** ad ki az Apache HTTP szervereket érintő, **nulladik napi** (zero-day) sérülékenységgel kapcsolatban, annak súlyossága és aktív kihasználása miatt.

A sérülékenység eredetileg [CVE-2021-41733](#) azonosító számon került nyilvántartásba, amely csak az Apache Server **2.4.49**-es verzióját érintette. A gyártó által kiadott első javítás (Apache HTTP Server **2.4.50**) sajnos nem bizonyult megfelelőnek, mivel egy újabb sérülékenységhez vezetett ([CVE-2021-42013](#)). A biztonsági hiba kivizsgálása során feltárássra kerültek **aktív kihasználásra tett kísérletek** is.

Az **NBSZ NKI haladéktalanul javasolja** az érintett verziókat futtató eszközökön a legújabb, **2.4.51** verziószámú frissítés telepítését – amely mindkét hibát javítja – valamint az alábbi, a támadásokkal összefüggésbe hozható IP címek tiltását a határvédelmi rendszeren.

Indikátorok (IoC):

134.122.112.12	143.198.136.88	161.35.188.242	161.35.86.181	167.99.133.28
162.241.114.189	162.241.69.182	185.246.210.169	94.46.15.22	69.49.228.92
69.49.235.93	3.83.56.46	141.101.146.162	156.146.50.105	156.146.50.98
185.254.96.162	185.56.80.11	194.126.177.17	192.3.194.202	89.248.173.143
80.239.140.67	47.106.92.240	45.77.138.50	45.86.203.97	27.102.114.78
14.161.74.29	149.28.140.81	185.98.87.200	217.138.216.4	142.93.153.4
178.128.172.249	79.165.90.196	51.79.142.118	59.12.193.82	64.39.106.120
64.39.98.36	45.155.204.183	34.223.64.22	35.82.51.168	37.237.230.28
44.242.181.147	45.146.164.110	145.220.25.28	165.227.79.155	161.35.215.189
143.198.62.76	174.138.42.66	46.101.59.235	137.184.69.137	165.227.125.18

TLP: WHITE



Hivatkozások:

- https://blog.talosintelligence.com/2021/10/apache-vuln-threat-advisory.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29
- https://httpd.apache.org/security/vulnerabilities_24.html
- <https://www.facebook.com/nki.gov.hu/posts/1404684166557504>



NEMZETI
KIBERVÉDELMI INTÉZET

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