Corero SmartWall® *Threat Advisory*

Hikvision SADP DDoS reflection/amplification new attack vector

Advisory ID: 03232022-1
Published: 23rd March 2022

Summary

The Corero SecureWatch Threat-Intelligence team has observed a new threat vector, leveraging **Search Active Device Protocol** (SADP) to launch a new type of reflective amplification DDoS attack.

SADP was intended for use on local networks to discover Hikvision devices, such as IP cameras and DVRs/NVRs. Its capabilities include viewing device information, activating devices, editing the network parameters of a device and resetting device passwords.

However, cybercriminals have now figured out that, with many Hikvision devices freely accessible across the Internet, they can abuse this protocol to launch damaging DDoS attacks.

Threat Vector

The attacker sends a small SADP request, using a spoofed source IP address of the victim, to UDP port 37020. The objective being to solicit the largest response possible from the exploited Hikvision device which it sends to the victim IP address, as a result of the spoofed source IP address used in the request.

Below is the request identified as triggering the largest amount of response data:

```
<?xml version="1.0" encoding="utf-8"?><Probe><Uuid>string</Uuid><Types>inquiry</Types></Probe>
```

With one 128-byte request, a response of 1,013 bytes can be generated – an amplification factor of 8x/790%

Recommended Action: SecureWatch Customers

SADP reflection/amplification attacks are exclusively from UDP port 37020. This attack traffic is detected and safely mitigated by SmartWall's automatic zero-day Smart-Rule protection.

SmartWall DDoS protection solutions mitigate a wide range of known and zero-day attacks, all while maintaining the availability of applications and services being protected and without disrupting the delivery of legitimate traffic. They are designed to handle large DDoS floods, reflective amplified spoof attacks (such as SADP), as well as attacks that are typically too low, or short, to be mitigated manually, or by traditional out-of-band solutions.

Corero customers using the latest software releases and recommended SmartWall protection settings are comprehensively defended from this increase in DDoS activity.

Please contact Corero Support if you have any questions.