FAQ: Command Injection Kwetsbaarheid

Wat is de command-injectie kwetsbaarheid?

Zoals vermeld in de officiële HSRC-202109-01 Security Notification van Hikvision, werd een Command Injection Kwetsbaarheid gevonden in de webserver van sommige Hikvision-producten. Door een ontoereikende input validatie, zou een aanvaller het lek kunnen misbruiken om een commando injectie aanval uit te voeren door het verzenden van een speciaal bewerkt bericht met kwaadaardige commando's.

Waar kan ik meer informatie krijgen?

1. De beveiligingskennisgeving van Hikvision. Hikvision heeft op 18 september een beveiligingskennisgeving gepubliceerd op haar website en op 19 september op sociale media-accounts.
2. Openbaarmaking rapport van de beveiligingsonderzoeker.

Is dit een achterdeur van de Chinese overheid?

Nee. Hikvision heeft geen achterdeuren van de overheid in onze producten. Watchful_IP, de beveiligingsonderzoeker die deze kwetsbaarheid aan Hikvision meldde, verklaarde: "Nee, absoluut NIET. Je zou het niet op deze manier doen. En niet alle firmware types zijn getroffen."

Wat heeft Hikvision gedaan om de kwetsbaarheid aan te pakken?

Hikvision volgt verantwoordelijke openbaarmakingsprincipes en het standaard Coordinated Vulnerability Disclosure Process dat algemeen wordt geaccepteerd in wereldwijde industrieën. Dit heeft betrekking op mechanismen waarmee kwetsbaarheden worden gedeeld en openbaar gemaakt op een gecontroleerde manier om de eigenaars en eindgebruikers van software het beste te beschermen.

Op 23 juni 2021 werd Hikvision gecontacteerd door een beveiligingsonderzoeker, genaamd Watchful IP, die een potentiële kwetsbaarheid in een Hikvision-camera meldde. Zodra we de ontvangst van dit rapport bevestigden, werkte Hikvision direct samen met de onderzoeker om de gemelde kwetsbaarheid te patchen en te verifiëren of de kwetsbaarheid met succes was verholpen.

Zoals de onderzoeker in zijn openbaarmakingsrapport opmerkte, was hij "verheugd te zien dat dit probleem op de aanbevolen manier was verholpen".

Nadat zowel het bedrijf als de onderzoeker zich ervan hadden vergewist dat het beveiligingslek door de bijgewerkte firmware op de juiste manier was verholpen, hebben we de beveiligingsmelding op 19 september op de website van het bedrijf en via sociale media vrijgegeven.

Wat is de aanbeveling van Hikvision met betrekking tot 'port forwarding'?

Een industrieblog heeft onlangs misleidende informatie gepubliceerd over de aanbeveling van Hikvision met betrekking tot 'port forwarding'. Let op, volgens de richtlijn van het bedrijf "Over Port Forwarding", waarschuwt Hikvision haar eindgebruikers tegen port forwarding, en adviseert dat "port forwarding alleen geconfigureerd moet worden wanneer dit absoluut noodzakelijk is."

Wanneer eindgebruikers ervoor kiezen om port forwarding te configureren voor apparaten die via het internet moeten worden benaderd, ondersteunt Hikvision de volgende best practices op het gebied van cybersecurity: (1) "minimaliseer de poortnummers die aan het internet worden blootgesteld", (2) "vermijd veelgebruikte poorten en herconfigureer ze naar aangepaste poorten" en "schakel IP-filtering in.", (3) Stel een sterk wachtwoord in, en (4) upgrade tijdig naar de nieuwste apparaatfirmware die door Hikvision is uitgebracht.

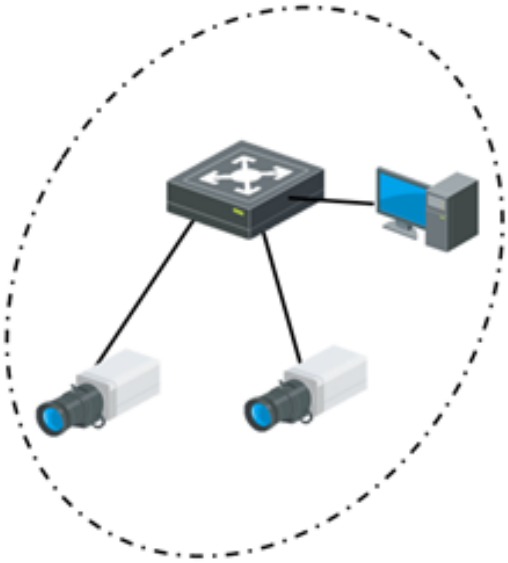
Hoe kan ik de risico's van mijn Hikvision-apparaten beoordelen?

Om deze kwetsbaarheid uit te buiten, moet een aanvaller zich in hetzelfde netwerk bevinden als het kwetsbare apparaat. Met andere woorden, als de aanvaller het inlogscherm van een kwetsbaar apparaat kan zien, zou hij het kunnen aanvallen. Als ze niet op het inlogscherm van een kwetsbaar apparaat kunnen komen, kunnen ze de kwetsbaarheid niet uitbuiten.

Om het risiconiveau van een kwetsbaar apparaat te evalueren, moet worden nagegaan of het getroffen model zijn http/https servers (meestal 80/443) rechtstreeks aan het Internet (WAN) blootstelt, wat een potentiële aanvaller de mogelijkheid zou geven om dat apparaat vanaf het internet aan te vallen. Hieronder staan enkele voorbeelden:

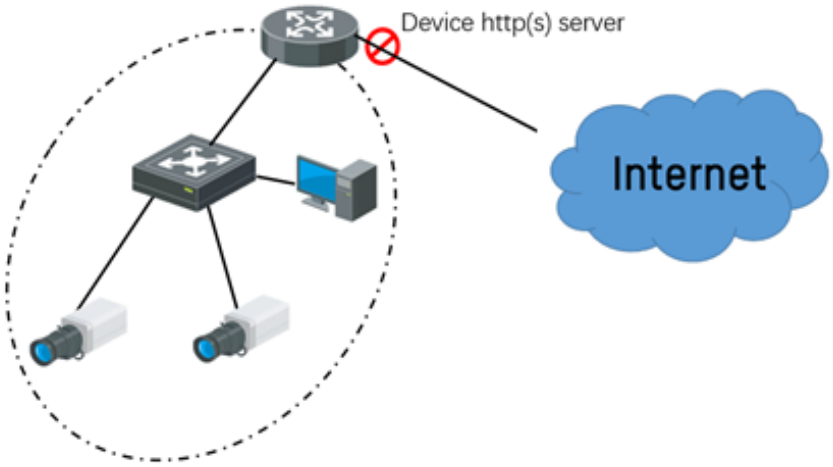
① LAN-netwerk zonder internettoegang (laag risico)

Potentiële aanvallers hebben geen toegang tot de webpagina van het apparaat vanaf het internet, dus het risico is laag (de aanvaller zou fysiek verbinding moeten maken met het LAN om toegang te krijgen).



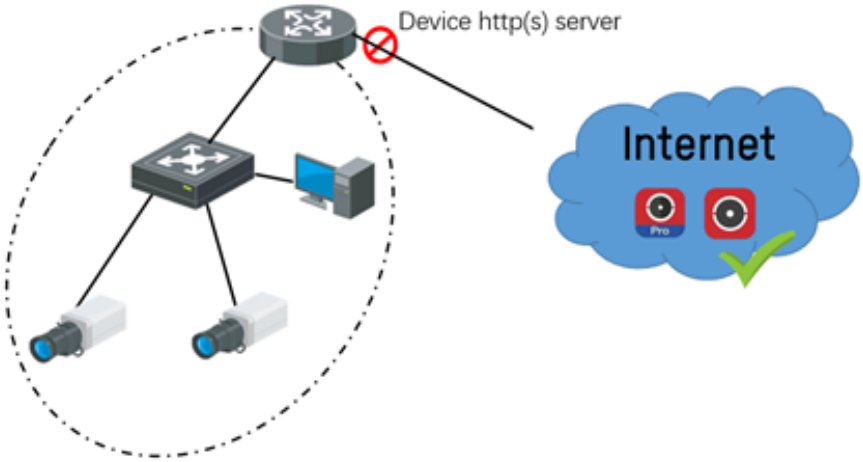
② WAN-netwerk met firewall die de http(s)-server van het apparaat blokkeert (laag risico)

Aangezien potentiële aanvallers nog steeds geen toegang kunnen krijgen tot de webpagina van het apparaat vanaf internet, wordt het systeem als laag risico beschouwd.



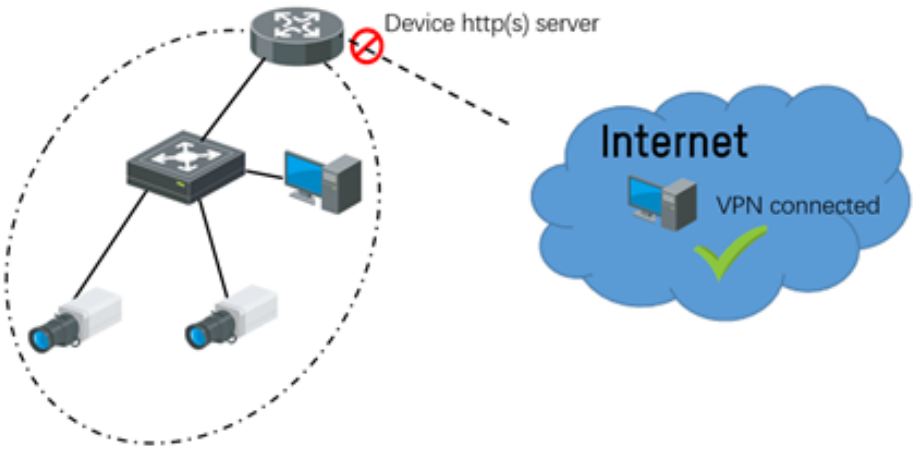
③ Hik-Connect & Hik-ProConnect (veilig & laag risico)

Hik-Connect en Hik-ProConnect zijn speciale gevallen binnen het tweede scenario hierboven. http(s) server is niet nodig in hun service, dus zijn ze net zo veilig als normaal.



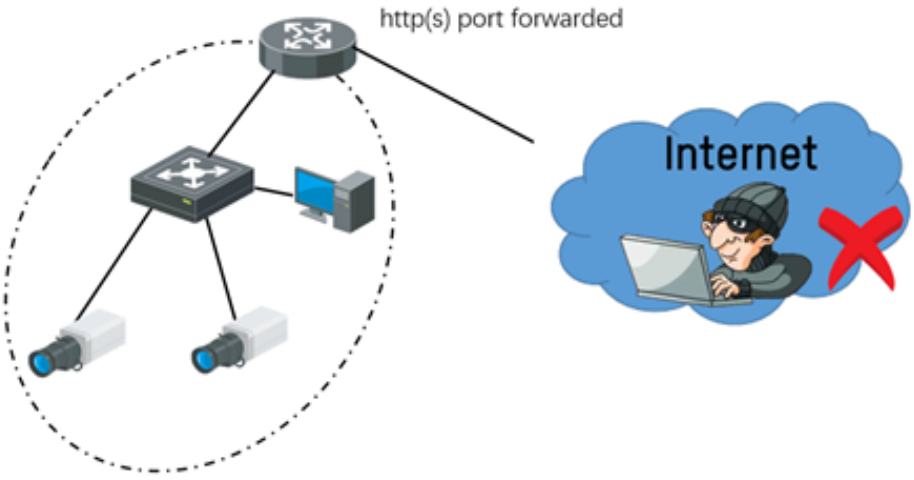
④ VPN toegang vanaf internet (laag risico)

Met VPN (Virtual Private Network) kunnen alleen geverifieerde gebruikers inloggen en toegang krijgen tot apparaten vanaf het sitenetwerk, dus het is een beveiligde manier om toegang te krijgen tot apparaten en niet gemakkelijk aan te vallen.



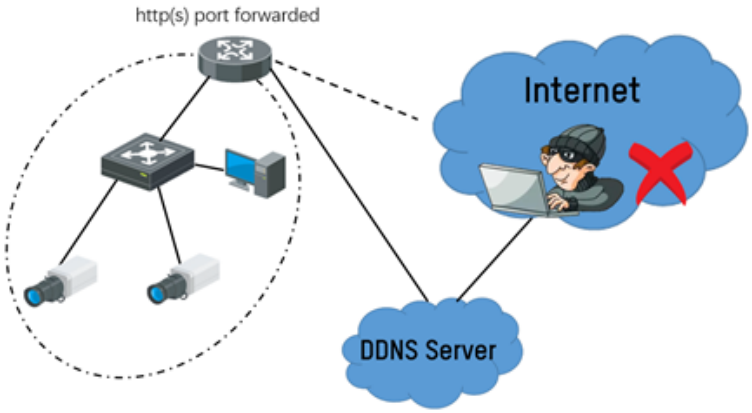
⑤ Port forwarding (hoog risico)

Port forwarding is een gemakkelijke en goedkope manier voor gebruikers om op afstand toegang te krijgen tot apparaten op de site. Dit brengt echter extra risico's met zich mee omdat het een open verbinding met het internet tot stand brengt. Door deze kwetsbaarheid ontstaat er een "toegangskanaal" waar potentiële aanvallers hun voordeel mee kunnen doen en loopt het systeem een hoog risico om aangevallen te worden.



⑥ DDNS (hoog risico)

DDNS is een speciaal geval van port forwarding, omdat het gewoon een omleidingsmethode is om toegang te krijgen tot apparaten zonder verificatie. In dit geval kan een potentiële aanvaller nog steeds toegang krijgen tot het IP/domein van een apparaat via het internet, waardoor het systeem een nog groter risico loopt.



⑦ Directe WAN-toegang (hoog risico)

Sommige sites installeren apparaten rechtstreeks op het internet (via WAN). Zolang zij een openbaar IP-adres en toegankelijke http(s)-poort hebben die blootgesteld zijn aan het internet, vormt het hele systeem een hoog risico.

Kortom, de eenvoudigste manier om het risiconiveau van een systeem te evalueren is te controleren of de webpagina van het apparaat rechtstreeks vanaf het internet (WAN) toegankelijk is, zonder extra netwerkverificatie. Zo ja, dan kan worden vastgesteld dat het systeem "een hoog risico" vormt.

Voor zover wij weten, is er momenteel geen publiek programma om deze kwetsbaarheid uit te buiten. Maar nu de patch is uitgebracht en aanvallers weten dat deze kwetsbaarheid bestaat, zullen ze ernaar op zoek gaan. Als u een getroffen camera/NVR hebt waarvan de http(s)-service direct aan het internet is blootgesteld, raadt Hikvision u sterk aan uw apparaat(en) onmiddellijk te upgraden naar de nieuwste versie die het beveiligingslek verhelpt of een veiligere oplossing te gebruiken, zoals een VPN.

Type	Platform	Firmware Type	Model Name	Firmware Version	Firmware Download URL
IPC	G3	IPC	DS-2CD2026G2-I DS-2CD2126G2-I DS-2CD2326G2-I DS-2CD2T26G2-2I/4I DS-2CD2626G2-I DS-2CD2626G2T-I DS-2CD2726G2-I DS-2CD2726G2T-I DS-2CD2046G2-I DS-2CD2146G2-I DS-2CD2346G2-I DS-2CD2T46G2-2I/4I DS-2CD2T46G2-ISU/SL DS-2CD2646G2-I DS-2CD2646G2T-I DS-2CD2746G2-I DS-2CD2746G2T-I DS-2CD2386G2-I(U) DS-2CD2T86G2-2I/4I DS-2CD2686G2-IZS DS-2CD2686G2T-IZ(S) DS-2CD2786G2T-IZ(S) DS-2CD2086G2-I(U) DS-2CD2786G2-IZS DS-2CD2H86G2T-IZS DS-2CD2H46G2T-IZS	V5.5.800 build210628	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/00%20%20Network%20Camera/00%20%20Product%20Firmware/G3%20platform%282XX6G2%203XX6G2%202XX7G2%202XX6G0%29/DS-2CD2XX6G2%2C2XX7G2%20Models/V5.5.800%20build210628
	G5	IPC	DS-2CD2043G2-I(U)(S) DS-2CD2143G2-I(U)(S) DS-2CD2343G2-I(U)(S) DS-2CD2T43G2-I(U)(S) DS-2CD2643G2-IZ(U)(S) DS-2CD2743G2-IZ(U)(S) DS-2CD2H43G2-I(U)(S) DS-2CD2023G2-I(U)(S) DS-2CD2123G2-I(U)(S) DS-2CD2323G2-I(U)(S) DS-2CD2T23G2-I(U)(S) DS-2CD2623G2-IZ(U)(S) DS-2CD2723G2-IZ(U)(S) DS-2CD2H23G2-I(U)(S) DS-2CD1083G0-I(U)(F) DS-2CD1183G0-I(U)(F) DS-2CD1383G0-I(U)(F) DS-2CD2046G2-I(U)(C) DS-2CD2046G2-IU/SL(C) DS-2CD2047G2-L(U)(C) DS-2CD2146G2-I(S)(U)(C) DS-2CD2147G2-(SU)(C) DS-2CD2346G2-ISU/SL(C) DS-2CD2346G2-I(U)(C) DS-2CD2347G2-L(U)(C) DS-2CD2646G2-IZSU/SL(C)	V5.5.801_210727	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/00%20%20Network%20Camera/00%20%20Product%20Firmware/G5%20platform%282xx3G2%202xx6G2%28C%29%202xx7G2%28C%29%203xx6G2%28C%29%203xx7G2%28C%29%201x83G0%29/2xxxG2%28C%29/V5.5.801_210727
PTZ	H5H3	IPDP	iDS-2DPxxxx-T4 iDS-2VPDxxx-T4	V5.5.800 build210628	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/01%20%20PTZ%20Camera/00%20%20Product%20Firmware/10%20PanoVu%28DS-2DPxxx%2C%20DS-2PTxxx%29/PanoVu%28DS-2DPxxxZIX-DE%28T4%29%29/V5.5.800%20build210628

IPC - Links to New firmware

Model Name	Firmware Version	Firmware Download URL
DS-7600NI-K1(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/05%20K-series/K1%28C%29/V4.31.102%20build210626
DS-7600NI-Q2(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/06%20Q-series/%5B76NI-Q1%28Q2%29%5D%28C%29/V4.31.102%20build210626
DS-7600NI-Q1(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/06%20Q-series/%5B76NI-Q1%28Q2%29%5D%28C%29/V4.31.102%20build210626
DS-7600NI-G2(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/06%20Q-series/%5B76NI-Q1%28Q2%29%5D%28C%29/V4.31.102%20build210626
DS-7100NI-Q1(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/06%20Q-series/%5B7100NI-Q1%28F1%29%5D%28C%29/V4.31.102%20build210626
DS-7800NI-F1(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/06%20Q-series/%5B7100NI-Q1%28F1%29%5D%28C%29/V4.31.102%20build210626
DS-7100NI-F1(C)	V4.31.102 build210626	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/02%20%20NVR/00%20%20Product%20Firmware/06%20Q-series/%5B7100NI-Q1%28F1%29%5D%28C%29/V4.31.102%20build210626

NVR - Links to New firmware

Type	Platform	Firmware Type	Model Name	Firmware Version	Firmware Download URL
Thermal Fixed Series	G5	IPTC	DS-2TD(12xx,26xx)/QA	V5.5.40_build20210720	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD%2812xx%2C26xx%29QA/V5.5.40_build20210720
Thermal Fixed Series	H7	IPTC	DS-2TD(11xx,12xx,21xx,23xx,26xx)P,PA	V5.5.42_build20210721	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD%2811XX%2C12XX%2C21XX%2C26XX%29P%2CPA%28With%20or%20Without%20T%29/V5.5.42_build20210721
Thermal Fixed Series	H3	IPHC	DS-2TD21xxV1 DS-2TD2137VP DS-2TD26xx DS-2TD28xx	V5.5.22_210702	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD21XXV1%2C2137VP%2C26XX%2C28XX/V5.5.22_210702
Thermal Fixed Series	H3	IPTCS	DS-2TD(12xx,26xx,28xx)V1	V5.5.22_210702	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD%2812XX%2C26XX%2C28XX%29V1/V5.5.22_210702
Thermal Fixed Series	H1	IPHC	DS-2TD21xx DS-2TD23xx DS-2TD24xx	V5.5.8_build20210702	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD21xx%2C23xx%2C24xx/V5.5.8_build20210702
Thermal PTZ Series	H5	IPTM	DS-2TD41xx-xx/W DS-2TD62xx-xx/W DS-2TD81xx-xx/W	V5.5.33_build210729	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD%2841xxW%2C62xxW%2C81xxW%29%20%28With%20or%20Without%20T%29/V5.5.33_build210729
Thermal PTZ Series	H3	IPTM	DS-2TD4xxx-xx/V2 DS-2TD62xx-xx/V2 DS-2TD81xx-xx/V2	V5.5.39_build210702	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/01%20Product%20Firmware/2TD%EF%BC%884xxxV2%2C%206xxxV2%2C%208xxxV2%29%20%28With%20or%20Without%20T%29/V5.5.39_build210702
Thermal Temperature Screening Series	H7	IPTC	DS-2TDxxxxB/P, /PA	v5.5.34 build210702	http://www.hikvisioneurope.com/portal/?dir=portal/Technical%20Materials/09%20%20Thermal/08%20Temperature%20Screening/00%20Product%20Firmware/01%20Baseline%20Firmware%20for%2012XXB%2C26XXB/v5.5.34%20build210702

Thermal - Links to New firmware