

**■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](https://www.exploit-db.com/exploits/39596)  [その他の複数のベンダの製品](https://www.exploit-db.com/exploits/39596) | https://lh6.googleusercontent.com/89C3dOtHy0UE_IregWq6OjUIYiyLvY7YdQH_GxBvL6CANr8U15c6jflTf-XddHLjefBvWi6ldpEnwofJXC0pbHqCX3MeStmzJLhxNxfe4r5YvdJ6ns-7lnIXIPNjJo0UXvBqUnnP |
| 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](https://seclists.org/fulldisclosure/2017/Jan/40)に類似) | https://lh4.googleusercontent.com/0gZ_ge7MQ8g15gqh5t_m-Aff-m7Vgd6dQ0jCLpwQoc4L1Rvepp4yKYWcnDJM9lH6SoYPxzE6bEOh2MB8I2ysXTLT-9GdzjMEHK6SdLI2KCGbOmw_u_lCTK5gqnslWKoHXX-kBuJS |
| [Huawei社製ルータ](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17215) | https://lh4.googleusercontent.com/Q1SNgG_jDcbQ0xXaNth6gPHpyhJ6WSb06v8O2AcgbJC9GWZwbdah1sZklVeplaN4H2lhCVRcuH703Lo3LkGcBqA6ie3LkDLpdBreojk5rSiGjFHXjMFkjeuH6kJXFSJKDdu6RluS |
| 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](https://www.exploit-db.com/exploits/46786)) | https://lh3.googleusercontent.com/aartPIV6SI2hLxdFQ5npNdK3fwZ_MIGTYUS9EtK6B-29J81Pv9QS2lKXgkZDGQcNDH_drJoknJGpOtWr651bwhp1XprVVihuna5fCsN93TO2jRP3zUTk3ySJSthBR61DNb7pO42y |
| [D-Link HNAP1](https://dl.packetstormsecurity.net/papers/attack/dlink_hnap_captcha.pdf) | https://lh6.googleusercontent.com/2JP1zbuIWPVsKkvnxm1bzPPt-6EuWQd99GA5-yOwwkCE5F8mUjXd8pGez3elF1YuTBecYLTKXoSTyRyoES3wf-99GPk39D8Ij-U1UJPZNlAn7DEeyVrJpwYoEREqtn2cbgUCO8SF |
| [Realtek SDK UPnP SOAP Command Execution](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8361) | https://lh4.googleusercontent.com/4Thn5hi22gI6l_6GuKPMqL0iCRPQ0YrRThUUz5eJIvclibbLu02WlQtO1fNVR9byAeIFwHQtbn03oZaEVFmC4Ioag61wQip126o4po4gDK9NisjrHWCd1OXR_nEaz14McmKt5Flr |
| [GPON80](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562) | https://lh5.googleusercontent.com/HFJvn9Q6ZIdZamo6aTPToy9q4mzCTAyhJQnoYlIVaSVGB6nCmbVjSK0otpMR5eVhJOrTKTcVbrZuCjsTMbOXOXYhx2lBEChQDjJpZbM-8o8XvVlzAE1Mfjuk9HlvteJp84-MfcfW |
| [GPON8080](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562) | https://lh3.googleusercontent.com/gtFCyhmtZsKs6LJEDdT-IGL2fI3zHU2-veTzkS6UU7T_9szYQCdp8_8eL6-Z8Z8rntEU4Aw1WBgsZfmC0v4cVAZeo-vQ_1k0_VJgvuEu_b_zm0FNiMDZcaUc8GZ8Fdsjl-EX-2nb |
| [GPON443](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10562) | https://lh6.googleusercontent.com/gd1i4B0st1IYlZ1cWsWaNV-SpDXqliEf_0Jd0byvntw-gF735o9cLRV770oqaqRBAfNuRBvxEX-ks4VAY0y9SQXjvezhOwglMH1W6qKJpFTg81bX13L099d4RBTxXEZJI_yfuuwZ |
| [JAWS Webサーバーの非認証シェルコマンドの実行](https://www.exploit-db.com/exploits/41471) | https://lh6.googleusercontent.com/jlWjBEil5Z4345Hy_W4WDppCD_WtYFuI5brr-32z_c99gRkghDloSt50v7CuGT2ufCO55Y7AUGb-RPXUdIyL6b2u258_CyF77T9riwBvCV3ULATLRCv_Ngz-hqgFAyvEJdg1ghPR |
| [Vacron NVR RCE](https://vulners.com/openvas/OPENVAS:1361412562310107187) | https://lh3.googleusercontent.com/iU17bWAiZhAslb5_-Xu10aLlqnceTqLaa2MAEqv_OF5Y8-ctR7Rjrz2TDym-_1C14Ml5vfNBfrkKOaRPr8jCsbsa3HBqsfc74g9J3JYu9uXmXEvwuOHZP4e3qCzl1NWXldroU9hY |
| UPnP SOAPコマンド実行(この[エクスプロイト](https://www.exploit-db.com/exploits/40740)に類似) | https://lh5.googleusercontent.com/SRQagm7S6XbCO2c5XY32Nw9d2RWfg8CcLzuKDzt5rJi7e-bevqPcxXje-q9b5luMTfzg9YEd4lJpjBlXdK2IUyewz4NofYT6qio3eek7U91KrkmYzqlNDGceZITxvNN7D5CA_Yy7 |
| [THINK-PHP](https://www.exploit-db.com/exploits/46150) | https://lh6.googleusercontent.com/8t0Eyo9vfms1K_twyt9zPBl_COKuUn6ZPNbWGXPVsb9MKG9XC8vSYDrgWQPBIgpfJjT9bB-tPrtovtBgSJiO636noH_M3yE_w03QbEncNM8Eh7aVhN1YxwExarJwZnsYrBBhCOdq |
| [HooTooTripMate RCE](https://www.exploit-db.com/exploits/46143) | https://lh4.googleusercontent.com/ZNmmk2QgOx-5Vf9duGlfaAHTtwixSA8OiTgfD5carPXMh7jKN2ky_frOG8EBetx3vGma0BpQl1_-_Vc_C39mQYexYbGQRL83bNRH0y7eSrH3GIJ-_7Qzrd3dj4g_U9eE9K5aOGFy |

# 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

