Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 19 januari 2024

Toegestane verspreiding: TLP:GREEN
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:GREEN en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Dit is de End of Week van vrijdag 19 januari. Deze week kleurde bijna heel Nederland voor de eerste keer in 2024 wit van de sneeuw. Gelukkig konden wij gewoon naar kantoor komen om deze End of Week voor u op te stellen!

In deze End of Week gaan we in op verschillende onderwerpen zoals de kwetbaarhedern in Ivanti die vorige week bekend zijn gemaakt, de toegenomen ransomware aanvallen in 2023 en een kwetsbaarheid in Opera's webbrowser.

Misbruik van kwetsbaarheden in Ivanti producten

Sinds afgelopen december heeft Ivanti actief misbruik van twee kwetsbaarheden waargenomen in Ivanti Connect Secure en Ivanti Policy Secure Gateways. Op 10 januari jongstleden zijn deze kwetsbaarheden door Ivanti openbaar gemaakt. Ivanti geeft aan dat alle ondersteunde versies van de eerdergenoemde software kwetsbaar zijn en geeft aan geen onderzoek te hebben gedaan naar niet-ondersteunde versies. Op dit moment is er nog geen patch voor de kwetsbaarheden, echter verwacht Ivanti deze vanaf komende week geleidelijk uit te kunnen brengen tot en met de week van 19 januari. Op dit moment is er een exploit publiek beschikbaar die ervoor zorgt dat de kans op misbruik enorm verhoogt. [1]

Ransomware-aanvallen enorm toegenomen in 2023

Niemand weet exact hoeveel ransomware-incidenten er precies plaatsvinden in een jaar. Omdat veel gevallen niet gerapporteerd worden, is het daadwerkelijke nummer van deze incidenten dat in een gegeven tijdsperiode plaatsvindt, onduidelijk. Echter, de ransomware-criminelen zelf plaatsen vaak wel de namen, industrieën en andere informatie over hun slachtoffers op hun data lek websites.

Tussen 2022 en 2023, is er een toename van bijna 73% in ransomware aanvallen te zien. In 2023 zijn er ruim 4600 incidenten geraporteerd. In 2022 was dit een stuk lager namelijk ruim 2600. Let wel: de hiervoor genoemde informatie is gebasseerd op de incidenten die zijn gedocumenteerd door de ransomware-groepen zelf.[2]

Remote code execution kwetsbaarheid gevonden in Opera's functie om bestanden te delen

Er is door het bedrijf Guardio Labs een kwetsbaarheid gevonden in de functie om bestanden te delen in de Opera webbrowser. De kwetsbaarheid zou het mogelijk maken om op afstand code uit te voeren. De functie om bestanden te delen genaamd My Flow zorgt ervoor dat gebruikers makkelijk berichten en bestanden kunnen delen tussen

[1] https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways

[2] https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/

hun desktop en mobiele apparaten, door simpelweg een QR-code te scannen met de mobiele applicatie van Opera. Zodra deze code is gescand krijgen gebruikers een soort chat die het mogelijk maakt om direct de gedeelde bestanden uit te voeren wat fijn is voor gebruikers, maar dat vormt ook een beveiligingsrisico.[3]

[3] https://labs.guard.io/myflaw-cross-platform-0-day-rce-vulnerability-discovered-in-operas-browsers-099361a808ab

Beveiligingsadviezen

Zie voor een actueel overzicht: www.ncsc.nl/actueel/beveiligingsadviezen

NCSC-2024-0018 [v1.00][M/H]	Kwetsbaarheden verholpen in Atlassian producten
NCSC-2024-0019 [v1.00][M/H]	Kwetsbaarheden verholpen in Citrix Netscaler ADC en Netscaler Gateway
NCSC-2024-0020 [v1.00][M/H]	Kwetsbaarheden verholpen in Google Chrome
NCSC-2024-0021 [v1.00][M/H]	Kwetsbaarheid verholpen in VMware Aria Automation
NCSC-2024-0022 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Database producten
NCSC-2024-0023 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Communications producten
NCSC-2024-0024 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle E-Business Suite
NCSC-2024-0025 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Enterprise Manager
NCSC-2024-0026 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Financial Services Applications
NCSC-2024-0027 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Fusion Middleware
NCSC-2024-0028 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Analytics
NCSC-2024-0029 [v1.00][M/H]s	Kwetsbaarheden verholpen in Oracle Hyperion
NCSC-2024-0030 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Java SE
NCSC-2024-0031 [v1.00][M/H]	Kwetsbaarheden verholpen iin Oracle JD Edwards
NCSC-2024-0032 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle MySQL
NCSC-2024-0033 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle PeopleSoft
NCSC-2024-0034 [v1.00][M/M]	Kwetsbaarheden verholpen in Oracle Siebel CRM
NCSC-2024-0035 [v1.00][M/H]	Kwetsbaarheden verholpen in Oracle Supply Chain producten
NCSC-2024-0036 [v1.00][L/H]	Kwetsbaarheden verholpen in Oracle Systems
NCSC-2024-0037 [v1.00][L/H]	Kwetsbaarheden verholpen in Trend Micro Deep Security

Wat was er nog meer in het nieuws

AndroxGh0st Malware wordt actief misbruikt.

AndroxGh0st is een met Python geschreven malware, ontworpen om informatie te extraheren uit applicaties gebasseerd op het Laravel-framework. Dit wordt specifiek gebruikt om de .env bestanden die gevoelige informatie bevatten zoals inloggegevens voor AWS, Office365, SendGrid en Twilio aan te bemachtigen.[4] Het Amerikaanse CISA heeft Indicators of Compromise online geplaatst.[5]

Foto's vrijgegeven van Colossus, eerste topgeheime computer

Ooit was hij zo topgeheim dat zelfs zijn monteurs niet wisten waar hij voor gebruikt werd. Maar op zijn tachtigste verjaardag mag de Britse inlichtingendienst GCHQ foto's delen van Colossus, het apparaat dat kan worden gezien als de eerste moderne computer.[6]

Openbaar Ministerie roept slachtoffers cybercrime op aangifte te doen

Het Openbaar Ministerie (OM) roept slachtoffer van cybercrime op om aangifte te doen. De huidige cijfers tonen een daling in het aantal meldingen, terwijl de trend de afgelopen jaren een stijgende lijn toonde.[7]

Honderd miljoen wachtwoorden toegevoegd aan Have I Been Pwned

Aan datalekzoekmachine Have I Been Pwned (HIBP) zijn honderd miljoen unieke wachtwoorden toegevoegd, alsmede 71 miljoen e-mailadressen van gecompromitteerde accounts. De inloggegevens werden onder andere door malware buitgemaakt en in een verzamelde dataset op internet aangeboden en gebruikt voor het uitvoeren van credential stuffing-aanvallen, aldus beveiligingsonderzoeker en HIBP-oprichter Troy Hunt.[8]

[4] https://fortiguard.fortinet.com/threat-signal-report/5066/androxgh0st-malware-actively-used-in-the-wild

[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

[6] https://nos.nl/artikel/2505346-foto-s-vrijgegeven-van-colossus-eerste-topgeheime-computer

[7] https://www.security.nl/posting/825469/Openbaar+Ministerie+roept+slachtoffers+cybercrime+op+aangifte+te+doen

[8] https://www.security.nl/posting/825853/Honderd+miljoen+wachtwoorden+toegevoegd+aan+Have+I+Been+Pwned

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

januari ’24

TLP:GREEN