TLP:WHITE

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor

augustus 2021

Maandelijks analyseert het NCSC de belangrijkste ontwikkelingen op het gebied van digitale veiligheid. Dit document beschrijft deze ontwikkelingen voor de maand augustus 2021. Naast de feitelijke ontwikkelingen zijn in dit document ook links naar de bronnen [🖱] en commentaren van het NCSC opgenomen. Zie de "NCSC Maandmonitor Bijsluiter" voor meer uitleg over dit product en de verspreidingsvoorwaarden.

Toename kwetsbaarheden in veiligheidskritische besturingssystemen

In het eerste halfjaar van 2021 nam het aantal publiek bekende kwetsbaarheden in industriële controlesystemen toe met 41 procent in vergelijking met het laatste halfjaar van 2020 volgens een rapport van Claroty. Van de 637 geïdentificeerde kwetsbaarheden kan 70 procent geclassificeerd worden als high of critical. [🖱1]

Een belangrijke bron voor deze gegevens is onderzoek van Microsoft dat sinds eind 2020 "BadAlloc" kwetsbaarheden heeft gevonden in tientallen softwarebouwstenen voor controle- en IoT-systemen. Die kwetsbaarheden kunnen worden misbruikt voor een denial-of-service-aanval of voor het uitvoeren van willekeurige code. [🖱2]

BlackBerry maakte op 17 augustus 2021 publiekelijk bekend dat ook zijn QNX Real Time Operating System (RTOS) de kwetsbaarheid bevat. Daarnaast was van VxWorks van Wind Wiver systems al bekend dat het was getroffen. QNX en VxWorks zijn de enige RTOS die zijn gecertificeerd voor veiligheidkritische taken in de lucht- en ruimtevaart, de auto-industrie en industriële veiligheid. Eerder publiceerde Schneider Electric al een waarschuwing voor kwetsbaarheden in de TRICONEX-veiligheidssystemen die zijn gecertificeerd voor het garanderen van de veiligheid van petrochemische en nucleaire processen. [🖱3] Andere recentelijk bekendgemaakte kwetsbaarheden betreffen onder andere Mitsubishi's veiligheids-PLCs, waardoor een aanvaller zich toegang kan verschaffen tot een systeem en andere beheerders kan uitsluiten. [🖱4]

Het verhelpen van dergelijke kwetsbaarheden is lastig omdat het vaak moeilijk is de besturingssoftware die kwetsbaarheden bevat te identificeren en te achterhalen welke leveranciers verantwoordelijk zijn voor het uitvoeren van patches. Ook zijn sommige systemen vanwege hun locatie moeilijk te bereiken, worden ze niet centraal beheerd of kunnen niet zomaar uitgeschakeld worden zonder lopende processen te hinderen. [🖱5] Dat het verhelpen van kwetsbaarheden in veiligheidskritische besturingssystemen complex is werd nog eens onderstreept door onderzoek van Armis, gepubliceerd in december 2020, met betrekking tot de URGENT/11 kwetsbaarheden. Hieruit bleek dat 97 procent van de kwetsbare eindproducten nog ongepatcht was ondanks dat Armis hier sinds 2019 voor waarschuwt. [🖱6] Soortgelijke kwetsbaarheden zijn NAME:WRECK, AMNESIA:33 en RIPPLE20. [🖱7] [🖱8]

- Het NCSC heeft voor de kwetsbaarheid in QNX een beveiligingsadvies opgesteld. De kwetsbaarheid is ingeschaald als medium-high. [🖱9]
- Het NCSC adviseert organisaties die gebruikmaken van OT-systemen contact te onderhouden met hun leveranciers en na te gaan welke systemen mogelijk kwetsbaar zijn en gepatcht moeten worden. Beperk toegang tot kwetsbare systemen en schakel waar mogelijk internetverbindingen uit.
- Zie voor verder advies het rapport "Succesfactoren voor digitaal veilige Operationele Technologie" van TNO in opdracht van het NCSC. [🖱10]
- Ook Nederlandse toezichthouders richten zich steeds vaker op cybersecurity issues zoals is te lezen in het in juni uitgebrachte eerste gezamenlijke inspectiebeeld cybersecurity vitale processen. [🖱11]

Microsoft Exchange: Proxy-kwartet

Tijdens BlackHat USA 2021 heeft een onderzoeker een presentatie gegeven over kwetsbaarheden in Microsoft Exchange. Tijdens onderzoek naar de serie kwetsbaarheden die eerder de naam ProxyLogon heeft gekregen, ontdekten onderzoekers een nieuw aanvalsoppervlak in Microsoft Exchange en vonden daarin nog 8 kwetsbaarheden. De kwetsbaarheden zijn gegroepeerd in drie mogelijke aanvalsmethoden: ProxyLogon, ProxyShell en ProxyOracle. [🖱12]

Voor de kwetsbaarheden die in deze aanvalsmethoden misbruikt worden, zijn sinds respectievelijk maart, april en juli van dit jaar updates beschikbaar. [🖱13] [🖱14] [🖱15] Misbruik van ProxyLogon en ProxyShell maakt overname van een Exchange-server mogelijk. Met ProxyOracle kan een kwaadwillende het wachtwoord van een gebruiker in plaintext uitlezen. [🖱16] [🖱17]

In de maandmonitor van maart dit jaar schreef het NCSC al over actief misbruik van de ProxyLogon kwetsbaarheden door de actor "HAFNIUM". In augustus verschenen er berichten dat er actief gescand wordt op Exchange-servers die kwetsbaar zijn voor ProxyShell, tevens is er misbruik waargenomen. [🖱18] [🖱19] Begin augustus en eind augustus is het high/high beveiligingsadvies met kenmerk NCSC-2021-0608 geüpdatet met nieuwe informatie. [🖱20] Op 31 augustus

heeft het NCSC ook via een bericht op de website een extra waarschuwing uitgebracht. [21] Het Amerikaanse Cybersecurity and Infrastructure Security Agency en het Nederlandse Digital Trust Center hebben in de maand augustus ook extra gewaarschuwd voor misbruik van de ProxyShell-kwetsbaarheden. [22] [23] Tot slot schreef het Zero Day Initiative eind augustus over een vierde 'nieuwe' kwetsbaarheid met de naam ProxyToken. Deze kwetsbaarheid maakt het mogelijk voor een kwaadwillende om zonder authenticatie toegang te krijgen tot e-mails van accounts. Voor deze kwetsbaarheid zijn reeds in juli updates beschikbaar gesteld. Het NCSC heeft deze kwetsbaarheid reeds meegenomen in het eerder genoemde beveiligingsadvies. [24] [25]

- Het feit dat er, ook in Nederland, nog steeds kwetsbare Microsoft Exchange-servers te vinden zijn terwijl er reeds enkele maanden patches beschikbaar zijn, geeft aan dat een adequaat patchbeleid helaas nog steeds niet de aandacht krijgt dat het verdient. Het NCSC publiceert dagelijks beveiligingsadviezen over kwetsbaarheden. Het is mogelijk, ook als u geen doelgroep bent, om u via een RSS-feed te abonneren.
- Met het nalaten van het tijdig installeren van beveiligingsupdates, is een organisatie onnodig kwetsbaar voor aanvallen. Criminelen gebruiken de ProxyShell kwetsbaarheden bijvoorbeeld om LockFile ransomware te installeren op Windows domeinen. [26]
- Het NCSC heeft Indicators of Compromise gedeeld via het Nationaal Detectie Netwerk.
- Het NCSC heeft doelgroeporganisaties en partijen uit het Landelijk Dekkend Stelsel die gebruikmaken van kwetsbare systemen genotificeerd.

Maandelijkse ontwikkelingen rondom ransomware

Onderwijsinstellingen lijken deze maand een gewild doelwit voor criminelen. Vanaf september zijn de scholen weer begonnen dit is voor criminelen een extra motivatie om daar een financieel slaatje uit te slaan. In het Verenigd Koninkrijk zijn zes scholen slachtoffer van ransomware geworden. [27] In Nederland is ROC Mondriaan getroffen door een aanval. Het is vooralsnog onbekend of het hier ransomware betrof. [28]
De FBI waarschuwt voor de groep 'OnePercent' die slachtoffers wist te maken via macro's in Word- en Excelbestanden. [29] In Australië, Chili, Italië, Taiwan en het Verenigd Koninkrijk is ransomwarevariant Lockbit 2.0 gedetecteerd. De actor heeft met name private partijen als doelwit en dreigt met het lekken van data indien geen betaling plaatsvindt. [30] [31] Naast deze twee criminele groepen is ook het relatief nieuwe ViceSociety deze maand actief. Zij richten zich vooral op kleine en middelgrote organisaties waarbij zij onder meer misbruik maken van de kwetsbaarheden in de Microsoft Printer Spooler-service van afgelopen periode. [32] [33]
Verder was er de afgelopen maand in het nieuws dat de groep Darkside (bekend van de aanval op Colonial Pipeline) volgens diverse beveiligingsbedrijven waarschijnlijk onder de naam BlackMatter een doorstart heeft gemaakt met het aanbieden van Ransomware-as-a-Service (RaaS). [34] [35] [36] Daarnaast zou de groep achter DoppelPaymer nu ransomware aanbieden onder de naam 'Pay or Grief'. [37]

- Zoals beschreven in het Cybersecuritybeeld Nederland (CSBN) van 2021, is en blijft ransomware een aantrekkelijk verdienmodel. Niet alleen criminelen, maar ook statelijke actoren kunnen ransomware inzetten. Ook werken criminelen en statelijke actoren in sommige gevallen samen. [38]
- Het blijft als organisatie belangrijk om bewust te zijn dat sommige sectoren een interessanter doelwit zullen zijn vanuit een crimineel perspectief. Denk bijvoorbeeld aan een hoge bankrekening, maatschappelijke impact bij uitval, gevolgen door ransomware zoals reputatieschade en dalende aandelen. Dit zijn diverse zaken die druk uitoefenen op de besluitvorming om mogelijk tot betaling over te willen gaan. Niemand wil zo'n besluit maken, zorg daarom dat uw organisatie voorbereid is op een ransomware-aanval. [39]
- Zorg onder andere dat de software op uw systemen up-to-date is en installeer updates direct wanneer deze beschikbaar zijn. Verouderde software maakt uw organisatie kwetsbaarder voor malware. Zie de recent uitgebrachte beveiligingsadviezen over onder andere de kwetsbaarheden in de Microsoft Printer Spooler-service. [40]

Pas waar mogelijk Zero Trust-principes toe

ICT-systemen worden traditioneel beveiligd vanuit een zogenaamde kasteelmentaliteit, wat resulteert in een infrastructuur met een enkele slotgracht. Dat heeft als belangrijk nadeel dat – wanneer aanvallers eenmaal binnen zijn – de systemen vaak weerloos zijn. Ook beschermt zo'n aanpak niet tegen aanvallen van binnenuit. De Zero Trust-filosofie komt aan deze bezwaren tegemoet. Afgelopen maand heeft het NCSC de factsheet 'Bereid u voor op Zero Trust' gepubliceerd. [41] In deze factsheet vraagt het NCSC aandacht voor de noodzaak van het toepassen van het Zero Trust gedachtengoed. Het NCSC adviseert organisaties de toepassing van Zero Trust-principes te verkennen, zodat fijnmazige netwerksegmentatie en identiteits- en toegangsbeheer mogelijk wordt gemaakt. Door het Zero Trust gedachtengoed mee te nemen bij vervangings- of uitbreidingstrajecten van uw IT-infrastructuur wordt het makkelijker en goedkoper om deze overstap te maken. Daarnaast is het lastig om dergelijke veranderingen – waaronder de verschuiving naar plaatsonafhankelijk werken en de adoptie van cloudtechnologie – op een veilige manier door te voeren als organisaties vast blijven houden aan een traditioneel ingerichte infrastructuur.

- Naast deze factsheet van het NCSC wordt ook de recente publicatie van NIST over dit onderwerp aanbevolen: 'Planning for Zero Trust architecture: a starting guide for administrators'. [42] NIST schetst hoe (de planning voor) een overstap naar Zero Trust aansluit bij generieke processen voor risicomanagement.

Overig nieuws Nederland

Wetsvoorstel uitbreiding bevoegdheden NCSC in consultatie [43] ■ Grapperhaus: politieorganisatie doelwit van Advanced Persistent Threats [44] ■ Provincie Gelderland gehackt: gegevens van 1600 ambtenaren mogelijk op straat [45] ■ Proef met dreigingsinfo voor individuele bedrijven [46] ■ Commissie: datalek toont dat controle coronatestbedrijven onvoldoende was [47] ■ AIVD wil ruimere wet voor digitale tegenaanvallen [48] ■ Cyberaanval op ziekenhuizen Apeldoorn en Zutphen, mogelijk persoonsgegevens bekeken [49] ■ Gehackt Haags mbo begint schooljaar met aangepaste lessen [50] ■ Nederlandse onderzoekers vinden kritieke lekken in back-upsoftware Vembu [51]