Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0272

Kwetsbaarheid verholpen in OpenSSH

2024-07-01 Revisie 2

Updates

Revision: 0

Initiele versie

Revision: 1

Typo's verwijderd.

Revision: 2

Er is Proof-of-Concept-code (PoC) verschenen die de kwetsbaarheid aantoont, gegeven voldoende tijd om de voorwaardelijke race-conditie uit te laten lopen. Handelingsperspectieven uitgebreid.

Toegestande verspreiding: TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE 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.firs t.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

Feiten

De ontwikkelaars van OpenSSH hebben een kwetsbaarheid verholpen in OpenSSH

Interpretaties

De kwetsbaarheid stelt een kwaadwillende in staat om zonder voorafgaande authenticatie willekeurige code uit te voeren met rechten van het sshd-proces. Het is niet uit te sluiten dat het ssh-proces met verhoogde rechten actief is, waardoor het mogelijk is dat de kwaadwillende code kan uitvoeren met rechten tot aan root.

De kwetsbaarheid bevindt zich in een beperkt aantal versies. Versies van OpenSSH 8.5p1 en hoger, tot 9.7p1 zijn kwetsbaar, en versies tot aan 4.4p1, welke niet meer ondersteund worden. Versies tussen 4.4p1 en 8.5p1 zijn niet kwetsbaar. Dit komt omdat de kwetsbaarheid een regressie is van de eerder verholpen kwetsbaarheid met kenmerk CVE-2006-5051, welke in versie 4.4p1 is verholpen, maar in versie 8.5p1 herintroduceerd is.

Daadwerkelijk misbruik is bijzonder ingewikkeld. Een kwaadwillende moet voor langere tijd connectiepogingen onderhouden. In een laboratoriumopstelling van de onderzoekers vereiste dat verbindingen van 6-8 uur, op 32-bit systemen. Theoretisch is het mogelijk om de kwetsbaarheid te misbruiken op 64-bit gebaseerde systemen, maar dat is nog niet aangetoond. Actief, grootschalig misbruik is hiermee dus onwaarschijnlijk.

Echter, vanwege de grote verspreiding en het brede gebruik van OpenSSH is het niet onaannemelijk dat bepaalde actoren, zoals de georganiseerde misdaad, ransomware-groepen of statelijke actoren, interesse in deze kwetsbaarheid krijgen en de energie investeren om werkende malware te bouwen.

Systemen met een actieve sshd-service, bereikbaar vanaf internet lopen het grootste risico. SSH is een populair protocol om op afstand systemen te beheren. Het verdient echter de afweging of de ssh-poort (standaard TCP poort 22, maar afhankelijk van de eigen installatie) actief en bereikbaar dient te zijn vanaf publieke netwerken.

Er is Proof-of-Concept-code (PoC) gepubliceerd die de kwetsbaarheid kan aantonen, indien aan bovengenoemde tijdsrestricties wordt voldaan. De PoC is toegespitst op een specifieke distro, hetgeen aannemelijk maakt dat de PoC niet zondermeer generiek en grootschalig inzetbaar te maken is, zonder substantiële investering in resources. Door de lange benodigde tijd, in combinatie met het gegeven dat de code voor een specifiek doelwit geschikt gemaakt moet worden, is grootschalig misbruik niet aannemelijk. Het publiceren van de PoC toont wel aan dat de kwetsbaarheid de aandacht heeft van onderzoekers, en daarmee ook eventuele kwaadwillenden.

Oplossingen

De ontwikkelaars hebben een nieuwe versie van OpenSSH uitgebracht, OpenSSH 9.8/9.8p1.

Eigenaars van systemen waarvan de SSH software in eigen beheer is kunnen de broncode downloaden en compileren. Leveranciers van Linux-distro's en systemen waarin OpenSSH in de firmware is geïmplementeerd zullen deze broncode moeten verwerken in nieuwe releases van distributie-packages of nieuwe firmware. Houd hiervoor de communicatie van uw leverancier in de gaten.

Indien upgrades op korte termijn niet in te zetten zijn, kan als workaround in de sshd-configuratie de variabele 'LoginGraceTime' op 0 gezet worden. Hiermee wordt de tijd waarin een loginpoging mag 'wachten' op nul gezet, waardoor misbruik van de kwetsbaarheid niet mogelijk is. De consequentie van deze maatregel is echter wel dat het sshd-proces gevoelig gaat worden voor een Denial-of-Service. Het NCSC adviseert hier een eigen risico-afweging te maken, waarbij in de afweging meegenomen moet worden of het in eerste instantie noodzakelijk is dat de ssh-service in kwestie publiek toegankelijk moet zijn.

Ook adviseert het NCSC om monitoring toe te passen op in gebruik zijnde SSH-services met een publieke toegang, en in de gaten te houden of herhaaldelijk sessies worden opgebouwd die uit hun gracetime lopen, de tijd waarin een login afgerond dient te zijn.

Het NCSC houdt de ontwikkelingen in de gaten en werkt dit beveiligingsadvies bij wanneer relevante ontwikkelingen zich voordoen.

Zie verder bijgevoegde referenties voor meer informatie.

Referenties

- https://www.openssh.com/releasenotes.html
- https://www.securityweek.com/millions-of-openssh-servers-potentially-vulnerable-to-remote-regresshion-attack/