ITSX

Understanding the Rules, the Players and the Tools

Madison Gurkha

Your Security is Our Business

Digitale achterdeuren in de Nederlandse internet infrastructuur

Onderzoek naar het gebruik van Simple Network Management Protocol (SNMP) op internet in Nederland

Ralph Moonen, CISSP
Directeur ITSX B.V.
SNMP paper final 0.9.docx
Version
24/10/2012

Inhoudsopgave

1 Samenvatting

In juli en augustus 2012 hebben ITSX en Madison Gurkha een onderzoek uitgevoerd naar de beveiliging van publiek benaderbare internet infrastructuurcomponenten in Nederland. Denk bij deze componenten bijvoorbeeld aan routers en modems die de toegang tot het internet mogelijk maken. Dit onderzoek heeft zich toegespitst op het gebruik van het, vaak vergeten, Simple Network Management Protocol (SNMP). Dit protocol wordt gebruikt om via het netwerk systemen te bewaken en te configureren. SNMP wordt veel op infrastructuurcomponenten gebruikt, en kent daardoor bijzondere beveiligingsconsequenties.

Hoewel SNMP veelal op interne netwerken wordt gebruikt, blijkt uit ons onderzoek dat in Nederland ook tienduizenden systemen publieke SNMP toegang aanbieden via internet waardoor hun configuratie kan worden uitgelezen. Van enkele duizenden systemen kan de configuratie door iedereen over internet zelfs worden gewijzigd, en daarmee kan een aanvaller de controle over deze componenten overnemen.

Onder deze systemen bevinden zich gevoelige componenten als routers, firewalls en servers, voornamelijk van midden- en kleinbedrijf maar ook van enkele grote bedrijven en overheidsgerelateerde organisaties. In het scenario dat deze componenten door een kwaadaardige aanvaller tegelijk en op afstand worden uitgeschakeld of overgenomen, kan dit leiden tot significante schade, zowel voor de individuele organisatie als wellicht ook de maatschappij.

Daarnaast kan toegang tot deze componenten worden misbruikt voor complexere aanvallen zoals het afluisteren van internetverkeer. Het verkrijgen van ongeautoriseerde toegang tot SNMP (via het internet) vormt hiermee een reeele bedreiging voor bedrijven en organisaties in Nederland en wij achten bewustwording hierover noodzakelijk, in combinatie met het nemen van de juiste maatregelen om problemen te voorkomen.

Ons onderzoek toont daarmee aan dat ondanks dat de problemen met SNMP al meer dan twintig jaar bekend zijn, kennelijk de risico's de ermee gepaard gaan onvoldoende aandacht krijgen van fabrikanten, service providers en beheerders.

2 Achtergrond

Vaak zijn door gezaghebbende instanties en onderzoekers uitspraken gedaan over de kwetsbaarheid van de internet infrastructuur in Nederland. Allen hebben daarbij gewaarschuwd voor grote zwakheden en de mogelijkheden voor aanvallers om schade aan te richten, of in te breken in systemen en netwerken. Enkele recente aansprekende voorbeelden en incidenten (bijvoorbeeld DigiNotar, Lektober, en het Dorifel/Citadel virus) hebben tot onderzoek geleid, maar dit is vrijwel altijd achteraf geweest, en de onderzoeken geven geen beeld van de staat van onze infrastructuur op dit moment.

2.1 Motivatie

Met ons onderzoek naar de beveiliging van SNMP in Nederland willen wij onze bijdrage leveren aan verdere bewustwording omtrent beveiliging in het algemeen en willen wij meer duidelijkheid geven over de specifieke beveiliging van mogelijk kritieke componenten in de Nederlandse infrastructuur.

2.2 Wat is SNMP?

SNMP is een hulpmiddel om apparaten mee te beheren. De status van een apparaat, inclusief foutmeldingen en instellingen, kan ermee worden opgehaald. Indien geactiveerd op het apparaat kunnen deze instellingen ook worden gewijzigd. Het ongeautoriseerd wijzigen van instellingen vormt een direct gevaar voor de vertrouwelijkheid, integriteit en beschikbaarheid van het apparaat.

Net zoals het protocol voor websites, het HyperText Transfer Protocol (HTTP), is het SNMP protocol gebaseerd op het netwerkprotocol internet Protocol (IP). Er bestaan vele simpele implementaties van SNMP, en er zijn vele tools beschikbaar voor SNMP, oa de Linux tools ‘snmpget’, ‘snmpset’, en ‘snmpwalk’. Ook grote enterprise suites zoals HP OpenView, IBM Tivoli en Nagios maken gebruik van SNMP. Het protocol verricht vaak op de achtergrond haar werk, en heeft bijna altijd toegang tot belangrijke systeeminstellingen. Hierdoor is het een interessant onderzoeksgebied, zowel voor hackers als onderzoekers.

Om de impact van een aanval met behulp van SNMP te kunnen bepalen hebben wij het publieke gebruik van SNMP (via internet) in kaart gebracht alsmede de aanwezige zwakheden in de beveiliging.

2.3 Het onderzoek en de testmethode

SNMP is een relatief onbekend protocol dat sinds 1988 is vastgelegd in internet Engineering Task Force (IETF) standaarden waaronder RFC1156. Het protocol is bedoeld om beheer van componenten op afstand mogelijk te maken. Hiertoe bestaan diverse implementaties en versies, te weten versie 1 t/m versie 3. Versie 1 is het meest gebruikt en wordt door alle besturingssystemen en zeer veel andere componenten zoals modems, printers, routers, switches, en videoconferentie apparatuur ondersteund. SNMP opereert op de applicatielaag en communiceert standaard via User Datagram Protocol (UDP) poort 161.

SNMP biedt toegang tot het Management Information Block (MIB). Hierin staan de operationele instellingen van een component zoals IP adressen, geconfigureerde interfaces, routeringstabellen en in veel gevallen ook zaken als geïnstalleerde software, patches, de procestabel van het besturingssysteem en systeemstatus. De toegang kan alleen-lezen zijn, of ook schrijven. In het request wordt dit aangegeven door het gebruik van de zg. 'community string'. Als de community string de waarde 'public' heeft, wordt alleen-lezen toegang verzocht. Als de community string de waarde 'private' heeft, wordt lees- of schrijftoegang verzocht. Bij het toelaten van schrijftoegang kan het beheer van de component volledig worden overgenomen. Bij alleen-lezen is de impact lager, maar kan alsnog gevoelige configuratie-informatie worden vrijgegeven. De waarde van de string kan vaak door de gebruiker zelf worden gewijzigd maar dit moet dan op alle apparaten gebeuren.

Uit diverse bronnen hebben wij een lijst opgesteld van alle IP blokken die in Nederland zijn toegewezen. Daarna hebben wij ruim de helft van deze IP blokken gescand op het publiekelijk aanbieden van UDP poort 161. Indien deze poort beschikbaar was, hebben wij het apparaat gevraagd zich te identificeren door middel van de '*alleen-lezen'* modus van SNMP. Indien het apparaat zich identificeerde, hebben wij daarna nogmaals aan het apparaat gevraagd of het zich wilde identificeren maar dan met de '*lees-en-schrijf'* modus van SNMP (waarmee instellingen kunnen worden aangepast). NB: Het daadwerkelijk wijzigen van instellingen is niet door ons getest in verband met mogelijke verstoringen en juridische aansprakelijkheden.

Indien lees- of lees-schrijftoegang mogelijk was, is tevens via '*whois'* in de RIPE-database onderzocht van wie het betreffende IP adres is. De gegevens zijn via scripts verzameld en geanalyseerd.

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C870
Software (C870-ADVSECURITYK9-M), Version 12.4(15)T10, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 14-Sep-09 23:35 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.568
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (536318451) 62
days, 1:46:24.51
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: XXXXXXXXXX
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 6
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

Voorbeeld 1: enige informatie uit een MIB

3 De resultaten

Onze resultaten laten zien dat in Nederland enkele tienduizenden apparaten op afstand uit te lezen zijn met SNMP[1]. Het gaat daarbij om een zeer grote verscheidenheid aan apparaten, veelal kleine consumentenapparatuur van particulieren zoals ADSL modems en WiFi routers. Maar tussen de resultaten bevinden ook een aanzienlijk aantal grote Nederlandse bedrijven, internetproviders en overheidsgerelateerde organisaties.

	Aantal	% van alle onderzochte IP's	% van gevonden IP's met SNMP
Onderzochte IP's in Nederland	25M+	100%	--
IP's met SNMP gevonden	15610	0.062%	100%
SNMP leesbaar	13656	0.055%	88.7%
SNMP schrijfbaar[2]	2294	0.0091%	14.7%

Tabel 1: aantal onderzochte IP's met SNMP toegang

Het uitlezen van (de MIB van) deze apparatuur voorziet een aanvaller van waardevolle informatie en is daarmee in sommige gevallen al ernstig genoeg. Sommige systemen geven bijvoorbeeld een overzicht van alle ontbrekende '*patches*'[3]. Met deze informatie kan een directe specifieke aanval worden opgezet.

```
HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "Windows Small Business Server
2003"
HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "Adobe Flash Player 11
ActiveX"
HOST-RESOURCES-MIB::hrSWInstalledName.3 = STRING: "Adobe Flash Player 10 Plugin"
HOST-RESOURCES-MIB::hrSWInstalledName.4 = STRING: "Adobe SVG Viewer 3.0"
HOST-RESOURCES-MIB::hrSWInstalledName.5 = STRING: "ATI Display Driver"
HOST-RESOURCES-MIB::hrSWInstalledName.6 = STRING: "Eaton Intelligent Power
Protector v1.26"
HOST-RESOURCES-MIB::hrSWInstalledName.7 = STRING: "Windows Internet Explorer 8"
HOST-RESOURCES-MIB::hrSWInstalledName.8 = STRING: "HP StorageWorks Library And
Tape Tools"
HOST-RESOURCES-MIB::hrSWInstalledName.9 = STRING: "Security Update for Windows
Server 2003 (KB2079403)"
HOST-RESOURCES-MIB::hrSWInstalledName.10 = STRING: "Security Update for Windows
Server 2003 (KB2115168)"
HOST-RESOURCES-MIB::hrSWInstalledName.11 = STRING: "Security Update for Windows
Server 2003 (KB2121546)"
HOST-RESOURCES-MIB::hrSWInstalledName.12 = STRING: "Security Update for Windows
Server 2003 (KB2124261)"
HOST-RESOURCES-MIB::hrSWInstalledName.13 = STRING: "Update for Windows Server
2003 (KB2141007)"
```

Voorbeeld 2: geinstalleerde windows patches van een Windows computer

[1] Wij hebben iets meer dan de helft van het aantal IP's in NL getest. Daarbij zijn 13656 resultaten geboekt. Het valt te verwachten dat in heel Nederland daarom rond de 25000 apparaten SNMP aanbieden op internet.
[2] Aanname hierbij is dat wanneer lezen met de 'schrijf-community-string' slaagt, dit betekent dat schrijven ook zou slagen hoewel wij dit niet daadwerkelijk hebben geprobeerd.
[3] Een patch is een door de fabrikant beschikbaar gestelde update die een security probleem met het apparaat oplost. Het ontbreken van een patch betekent een lek in het systeem.

Het gevaar wordt nog groter als ook schrijven mogelijk is; het op afstand kunnen aanpassen van instellingen is een ernstige zwakheid. Met het schrijven van de MIB is het mogelijk het apparaat op afstand te beheren. Met beheren wordt hier bedoeld het naar wil kunnen aanpassen van alle instellingen van het apparaat.

In sommige gevallen zijn met schrijfrechten zeer geavanceerde aanvallen mogelijk. Zo is het bij de meeste apparatuur van Cisco en andere grote leveranciers van netwerkapparatuur mogelijk om met schrijftoegang tot de MIB, een geheel nieuwe configuratie in het apparaat te laden. Deze configuratie kan alle functies van het apparaat naar de hand van de aanvaller zetten. Een mogelijke uitwerking van een dergelijke aanval is hierbij bijvoorbeeld het aftappen van alle netwerkverkeer dat door deze router heen getransporteerd wordt (zie Phrack magazine #56, article 0xa).

Een gerichte aanval op de routers en firewalls van een bedrijf of organisatie zou potentieel een zeer grote impact kunnen hebben omdat alle netwerkverkeer afgeluisterd zou kunnen worden.

Een destructievere mogelijkheid is het simpelweg uitzetten van het apparaat (vaak mogelijk in combinatie met het uitsluiten van de daadwerkelijke beheerder of eigenaar waardoor deze de toegang wordt ontzegd).

Gezien de eigenaars en hoeveelheid van de apparaten die schrijftoegang toestaan, is deze laatste mogelijkheid zeer schadevol. Zeer veel midden- en kleinbedrijven zouden voor enige tijd van alle internettoegang afgesloten zijn, en potentieel duizenden particulieren zouden een beroep moeten doen op de servicemonteur van de internet Service Provider (ISP) om de apparatuur te resetten.

4 Enkele scenario's

Gebaseerd op onze resultaten en de gedocumenteerde mogelijkheden van de aangetroffen apparatuur geven wij enkele voorbeelden van mogelijke aanvallen.

1) *Massale verstoring van internetverkeer in Nederland*

Van alle duizenden apparaten die dit toestaan, worden de interfaces uitgezet of van een ander IP adres voorzien (hierdoor kunnen apparaten niet meer bereikt worden). Tevens wordt waar mogelijk de legitieme beheerder buitengesloten.

Naar schatting tienduizenden achterliggende apparaten in Nederland houden hierdoor op te functioneren omdat zij niet langer met het internet kunnen communiceren. De beheerder zal fysiek naar alle apparaten moeten gaan om deze te resetten. Deze aanval is zeer eenvoudig op te zetten door een aanvaller met middelmatige kennis van internet en protocollen.

2) *Afluisteren netwerkverkeer*

Complexe netwerkcomponenten met veel functionaliteit zoals bijvoorbeeld Cisco routers kunnen opnieuw worden geconfigureerd waarbij gebruik gemaakt wordt van geavanceerde technieken zoals het opzetten van Generic Routing Encapsulation (GRE) tunnels. Hierna kan al het verkeer worden omgeleid en afgeluisterd. Deze complexere aanval is o.a. beschreven in artikelen in publicaties zoals *Phrack* #56 en daarmee goed uitvoerbaar voor een aanvaller met enige kennis van zaken.

3) *Man-in-the-Middle aanvallen*

Veel netwerkcomponenten zoals ADSL modems staan het wijzigen van het IP adres van de Domain Name System (DNS) server toe via SNMP. Indien dit IP adres wordt gewijzigd naar een IP adres dat onder controle van de aanvaller staat, kunnen DNS queries worden onderschept en kunnen connecties van achterliggende systemen naar het internet worden onderschept.

Dit type DNS aanval wordt regelmatig gebruikt door internetcriminelen om bankgegevens te onderscheppen, maar de mogelijkheid dit via SNMP uit te nutten is niet eerder beschreven.

4) *Hack aanval gebruik makend van informatie uit de MIB*

De MIB bevat zeer veel gedetailleerde informatie. Bij sommige oudere Windows systemen bijvoorbeeld een complete lijst van alle gebruikers op het systeem en de geïnstalleerde patches en fixes. Met deze informatie is soms een directe aanval op te zetten maar ze is ook bruikbaar om een '*social engineering'* aanval mee op te zetten.

5) Diefstal of inbraak

Onder de apparaten die schijftoegang en dus het aan- en uitzetten ervan toelieten bevond zich ook beveiligingsapparatuur (onder meer beveiligingscamera's en winkeldetectiepoortjes). Door het uitzetten van deze apparatuur via SNMP kan fysieke inbraak of diefstal worden gefaciliteerd.

5 De cijfers

Wij hebben uit twee verschillende Geo-IP databases een lijst samengesteld van IP adresblokken die in Nederland gebruikt worden. In totaal gaat het om ruim 45 miljoen IP adressen. Hiervan hebben wij er ruim 25 miljoen gescand.

Op 13.610 apparaten bleek uit onze scan UDP-poort 161 open te zijn. Van deze apparaten antwoordden 13.656 op alleen-lezen verzoeken en 2294 op lees- en schrijfverzoeken.

Alleen lezen

Van de apparaten die alleen-lezen toegang publiekelijk toestaan, identificeren ruim 3000 apparaten zichzelf als midden- en kleinbedrijf ADSL modems van alle grote Nederlandse ISP's.

Onder de identificaties bevinden zich tevens ruim 800 routers van diverse fabrikanten zoals Cisco en Juniper. Dit zijn professionele routers, met veel complexe functionaliteit. De informatie in de MIB van deze apparaten kan zeer waardevol zijn voor aanvallers omdat zij onder andere interne IP adressen, MAC adressen, interface configuraties, routeringstabellen en filterinstellingen bevatten.

Ook ongeveer 960 Linux en 172 Windows servers lieten zich remote uitlezen. Andere devices zijn bijvoorbeeld 170 Uninterruptable Power Supplies (UPS) en 67 Tandberg Videoconferentie apparaten.

Schrijven

Als we kijken naar de apparaten die niet alleen lezen maar ook schrijftoegang lijken toe te staan, gaat het om een veel kleiner percentage van de apparaten. 15% van alle devices met SNMP laten zich schrijven. Echter omdat schrijftoegang het remote beheer van de apparaten toestaat - inclusief het aan- en uitzetten en wijzigen van de configuratie - is de impact hiervan vele malen hoger.

Het gaat hierbij om tussen de 900 en 1000 door ons geidentificeerde ADSL routers van voornamelijk midden- en kleinbedrijf, maar ook enkele grotere bedrijven. Dit betekent dat in Nederland in zijn geheel meer dan 1500 midden- en kleinbedrijven zeer eenvoudig door een aanvaller van het internet kunnen worden afgesloten.

Van de professionele netwerkapparatuur hebben wij 134 routers en 40 Virtual Private Network (VPN) servers geïdentificeerd die zich remote laten overnemen. Hierbij gaat het vaak om middelgrote tot grote bedrijven. Saillant detail is dat VPN servers een beveiligingscomponent zijn. Het feit dat deze over te nemen zijn is daarom des te risicovoller.

6 Oorzaken

SNMP is dus aantoonbaar een risico voor een groot deel van de gebruikers, terwijl deze risico's al meer dan twintig jaar bekend zijn. Op de vraag wiens verantwoordelijkheid dat is, zijn verschillende antwoorden mogelijk die te maken hebben met de dieperliggende oorzaken van het onveilig gebruik van SNMP. Wij onderkennen een aantal oorzaken:

- Consumenten apparatuur zoals routers en modems waar SNMP standaard aan staat, maar die niet ontworpen zijn om een directe internet-verbinding te hebben, zijn niet afgeschermd als ze toch direct aan internet worden verbonden. Dit komt voor als consumenten zelf apparatuur aanschaffen en onveilig aansluiten of wanneer ISP's on veilig geconfigureerde apparatuur uitleveren aan klanten.
- Configuratiefouten af fabriek: sommige routers en modems die wel ontworpen zijn om een directe internet verbinding te hebben zijn door de fabrikant onveilig geconfigureerd. Deze worden door bedrijven of consumenten onterecht als veilig beschouwd.
- Configuratiefouten door beheerders: omwille van gemak of door onkunde wordt bij professionele producten SNMP bewust aangezet door de eigenaar of beheerder zonder bewust te zijn van de risico's.

Het is duidelijk dat de verantwoordelijkheid niet bij een partij te leggen is, maar dat consumenten, bedrijven, ISP's en fabrikanten allen een rol spelen.

7 Mogelijke maatregelen

De internet providers zijn in veel gevallen verantwoordelijk voor het configureren van de apparatuur die bij klanten wordt geplaatst. Dit betekent dat zij het eerst aanspreekpunt zijn voor verbetering van de huidige beveiliging, het voorlichten van klanten het voorkomen van toekomstige gebreken. Om deze reden hebben wij alle geidentificeerde ISP's aangeschreven en hen voorzien van onze gedetailleerde resultaten. Alle aangeschreven ISP's hebben ons laten weten maatregelen te hebben getroffen voor publicatie van dit artikel.

Tevens bestaat kennelijk bij veel (netwerk)beheerders weinig bewustzijn over de mogelijke gevaren van SNMP. Het feit dat SNMP uberhaupt over internet gebruikt wordt is al een risico. Apparaten die SNMP nodig hebben zouden achter een firewall moeten staan, of alleen SNMP verzoeken van bekende bronnen moeten toestaan.

Fabrikanten van apparatuur gaan ook niet vrijuit in deze kwestie. Apparatuur krijgt vaak de verstekwaarde 'SNMP aan' mee, zonder dat dit duidelijk aan de klant wordt gecommuniceerd of ook maar in de handleiding vermeld staat. Vrijwel alle merken printers en ook veel WiFi access points zijn op deze manier geconfigureerd en zijn niet bedoeld om rechtstreeks met internet verbonden te zijn.

Maatregelen kunnen dan ook bestaan uit een combinatie van de volgende aspecten:

- Het uitzetten van SNMP indien dit niet wordt gebruikt.
- Het vergroten van het bewustzijn van consumenten, fabrikanten en ISP's.
- Het wijzigen van standaardinstellingen van apparaten af fabriek.
- Het plaatsen van de componenten achter de internet router of firewall in plaats van direct aan het internet gekoppeld.
- Het afschermen en/of filteren van SNMP-verzoeken in firewalls (wijzigen van de netwerkconfiguratie).
- Het wijzigen van de community-string van de apparatuur. Indien de aanvaller de community-string waarde niet kent, kan de MIB niet worden uitgelezen. In veel gevallen kan de community-string worden gewijzigd.

8 Beperkingen

Ons onderzoek kent een aantal beperkingen die de resultaten kunnen beinvloeden. Echter, al deze beperkingen betekenen dat wij niet alles hebben gevonden dat er is.

Het eerste voorbehoud is het feit dat wij gebruik hebben gemaakt van een zogenaamde 'stateless' scanner' [4] en dat SNMP het onderliggende transportprotocol UDP gebruikt. UDP is een inherent onbetrouwbaar protocol. De combintie met een stateless scanner maakt het zeer waarschijnlijk dat wij maar een deel van de werkelijke hoeveelheid apparaten die SNMP gebruiken hebben gevonden. Het UDP protocol in combinatie met stateless scanners is niet betrouwbaar maar omwille van tijdsbeperkingen hebben wij toch hiervoor gekozen. De grootte van deze afwijking is niet vast te stellen, maar als deze bestaat dan hebben wij te allen tijden minder gevonden dan werkelijk aanwezig.

Bij het bepalen van het type apparaat en de eigenaar ervan, zijn wij uitgegaan van het antwoord van het apparaat zelf, en de gegevens zoals beschikbaar bij RIPE, opgevraagd door middel van het 'whois' commando. Deze gegevens zijn niet noodzakelijkerwijs altijd correct, maar het is onze ervaring dat de afwijking hierin hoogstens enkele procenten is.

Met betrekking tot het schrijven geldt dat dat het mogelijk is dat een apparaat antwoordt als de 'private' community string wordt gebruikt, maar niet daadwerkelijk over te nemen is. Omdat wij het daadwerkelijk schrijven naar de MIB niet hebben getest, is hierdoor een afwijking in de resultaten mogelijk. Echter, gezien de consistentie van implementatie van SNMP over verschillende apparaten die wij in gecontroleerde omstandigheden hebben getest, waarbij wel is geschreven, is het onwaarschijnlijk dat dit een significant deel van de resultaten zal beïnvloeden.

Als laatste beperking geldt dat wij slechts iets meer dan de helft van de in Nederland geregistreerde IP adressen hebben benaderd. Voor de conclusies van ons onderzoek is dit echter irrelevant omdat een 'steekproef' van 50% sowieso representatief is.

[4] De gebruikte scanner was 'unicornscan'