NOX Security Whitepaper

Version 17.0
19-03-2024

Innehåll

Introduktion till NOX Software releases

EOL System software

Software release ≤R6 är End-of-life, och varken supporteras eller uppdateras av NOX Systems.

Det rekommenderas att uppdatera NOX CPUer till R8 (11.xx) för att säkra nyaste säkerhetsteknologin, samt fortsatt support och uppdatering.

Gäller från systemversion R7

NOX central programvara är designad för att uppfylla de senaste IT-säkerhetsstandarderna.

För detta ändamål är all dataöverföring krypterad (förutom NOX TIO-enhet) och anslutningen autentiseras på nätverkslagret.

Dessutom måste användaren autentisera sig till systemet med en användarkod eller användarnamn/lösenord.

Om centralenheten med lagrade data hamnar i obehöriga händer kan data som lagras på CPU inte läsas utan giltig autentisering.

Säkerhetsåtgärder:

- Användning av TLS 1.2
- Skydd mot brute force attacker
- Skydd mot man-in-the-middle-attacker
- Valfria kundspecifika certifikat för TLS-autentisering
- Konfigurationsdata i CPU:n lagras krypterad
- Systemfiler i CPU:n kontrolleras för giltighet med hjälp av kryptering
- PC-applikationer använder kodsignering

Rekommendationer för högsäkerhetsinstallationer (klass 3 och 4)

- Användning av SL4 (autentisering med användarnamn och lösenord)
- Använda ett lösenord för att se konfigurationen
- Användning av komplexa lösenordsregler
- Aktivering av endast nödvändiga nätverkstjänster i systemet
- Ingen användning av NOX TIO-enheter med kontrollfunktioner (ingen kryptering)
- Begränsning av användargränssnitt till vad som är absolut nödvändigt
- Användning av tidsprofiler för att begränsa användarens giltighet

NOX och SIMS, vanligaste använda portar

Riktning	Applikation	Beskrivning	Från	Till	Port	Konfigurerbar	Säkerhet	Default
NOX Ingående								
	NOX Config	Generell System Konfiguration	Software	Central	4322	Nej	Krypterad	Öppen
	NOX Config	NOX Loader	Software	Central	6251	Nej	Krypterad	Öppen
	NOX Config	Terminal Window	Software	Central	4321	Nej	Krypterad	Öppen
	NOX PC Control	Användargränssnitt for Windows PC	Software	Central	4322	Nej	Krypterad	Öppen
	NOX PC TPA	Användargränssnitt för Touch skärm med grafik	Software	Central	4322	Nej	Krypterad	Öppen
	NOX SmartPhone App	Användargränssnitt för SmartPhones och MacOS	Software	Central	4325	Ja	Krypterad	Stängd
	NOX SSH Server	Användargränssnitt för simpla integrationer	Software	Central	22	Ja	Krypterad	Stängd
	NOX Modbus Server	Integration med HVAC/CTS System	Software	Central	502	Ja	Ingen	Stängd
	NOX SNMP Trap Reciever	SNMP trap mottagare från utvalda Communities	Software	Central	162	Nej	Ingen	Stängd
	NOX TIO	Användargränssnitt Telnet/Text	Software	Central	4001	Ja	Ingen	Stängd
	NOX in Netvork Configration	Flera NOX Centraler i samma nätverk	Undercentral	Huvudcentral	8981	Nej	Krypterad	Stängd
NOX Utgående								
	NTP	Tidssynkronisering via NTP Server	Central	Service	123	Nej	Ingen	Stängd
	Modbus Client	Integration med HVAC/CTS Systemer	Central	Service	502	Ja	Ingen	Stängd
	SMTP	Email-utskick från NOX centralen	Central	Service	587	Ja	Krypterad	Stängd
	NOX SmartPhone App	NOX Push notifications: push.noxsystems.com	Central	Service	4324	Nej	Krypterad	Stängd
	NOX TIO	Användargränssnitt Telnet/Text	Central	Service	4001	Ja	Ingen	Stängd
	SmartIntego	Trådlösa dörrar till NOX	Central	Gatenode	2101	Nej	Ingen	Stängd
	SIA IP	Alarmtransmission	Central	KC	30001	Ja	Valfri	Stängd
SIMS Ingående								
	SIMS Client	Klient till styrning av SIMS-anslutna NOX Centraler	Client PC	SIMS Server	2010	Ja	Krypterad	Öppen
SIMS Utgående								
	SIMS Server	Förbindelse till NOX Centraler	SIMS Server	Central	4322	Nej	Krypterad	Öppen
	NOX License Server	NOX Systems Licens server: license.noxsystems.com	SIMS Server	Service	8777	Nej	Krypterad	Öppen

NOX BUS

NOX-bussen är av typ RS-485 Standard.

NOX-bussen använder obfuskering av data vid kommunikation mellan CPU och NOX-enheter, utvecklad av NOX Systems.

Alla meddelanden ändrar form från gång till gång vilket gör det mycket komplicerat att behöva simulera/emulera ett meddelande och spela upp det på NOX-bussen.

NOX-bussen är en del av NOX-systemet och har inget inflytande på IT-infrastrukturen, den utförs som en fristående del av själva NOX-installationen.

Om bussen avbryts kommer NOX-systemet att generera ett sabotagelarm för alla saknade enheter.

När man försöker manipulera datapaket kommer dessa att ignoreras eftersom de inte innehåller korrekt datastruktur.

NOX-center i nätverk

NOX i nätverksförhållanden består av 2 eller flera NOX-processorer som kommunicerar via TCP/IP.

Kommunikationen är skyddad med en 384-bitars Blowfish-kryptering i alla Firmware-versioner till och med version 9.85.

Från R7 (version 10.0) används 256-bitars AES-kryptering.

Kommunikation sker på följande portar: 8981

Porten är låst och kan inte ändras.

NOX Redundant CPU

NOX Redundant CPU består av 2 NOX CPU:er som kommunicerar via TCP/IP, de dupliceras 1-till-1, och delar fysiska bussar, så att när den ena startar om eller kraschar tar den andra över utan avbrott. All kommunikation mellan primär och sekundär CPU sker utan kryptering.

Kommunikation sker på följande portar: 8982

NOX PC Control

NOX PC Control är ett operativsystem som kan komma åt NOX CPU via TCP/IP.

Kommunikationen är skyddad med en 384-bitars Blowfish-kryptering i alla Firmware-versioner till och med version 9.85

Från R7 (version 10.0) används 256-bitars AES-kryptering.

Från version 10.0 är det möjligt att välja högre säkerhet genom certifikatbaserad autentisering, eller autentisering med användarnamn och lösenord.

Programvaran kan installeras på alla Windows-versioner, 32 bitar och 64 bitar, från Windows 7 och framåt.

Förutsättningen för fullt fungerande programvara är förinstallation av .NET 2.0 (ingår i .NET 3.5.1)

Kommunikation sker på följande portar: 4322

Porten är låst och kan inte ändras.

NOX PC TPA

NOX PC TPA är ett operativsystem som kan komma åt NOX CPU via TCP/IP.

Kommunikationen är skyddad med en 384-bitars Blowfish-kryptering, i alla Firmware-versioner till och med version 9.85

Från R7 (version 10.0) används 256-bitars AES-kryptering.

Från version 10.0 är det möjligt att välja högre säkerhet genom certifikatbaserad autentisering, eller autentisering med användarnamn och lösenord.

Programvaran kan installeras på alla Windows-versioner, 32 bitar och 64 bitar, från Windows 7 och framåt.

Förutsättningen för fullt fungerande programvara är förinstallation av .NET 2.0 (ingår i .NET 3.5.1)

Kommunikation sker på följande portar: 4322

Porten är låst och kan inte ändras.

NOX Logger

NOX Logger är en mjukvara som kan köras oberoende av NOX Config eller NOX PC Control, funktionerna i detta program är att samla in loggar i realtid genom NoxDLL.dll.

Kommunikationen är skyddad med en 384 bitars Blowfish-kryptering i alla Firmware-versioner upp till och inklusive version 9.85 (NOX Logger 3.0)

Från R7 (version 10.0) används 256-bitars AES-kryptering.

Från version 10.0 är det möjligt att välja högre säkerhet genom certifikatbaserad autentisering, eller autentisering med användarnamn och lösenord. (NOX Logger 4.0)

Programvaran kan installeras på alla Windows-versioner, 32 bitar och 64 bitar, från Windows 7 och framåt.

Förutsättningen för fullt fungerande programvara är förinstallation av .NET 2.0 (ingår i .NET 3.5.1) och följande filer måste finnas med i mappen med NOX Logger:

Kommunikation sker på följande portar: 4322

Porten är låst och kan inte ändras.

NOX Config

NOX Config är konfigurationsprogram som kan komma åt NOX CPU via TCP/IP.

Kommunikationen är skyddad med en 384-bitars Blowfish-kryptering i alla Firmware-versioner till och med version 9.85

Från R7 (version 10.0) används 256-bitars AES-kryptering.

Från version 10.0 är det möjligt att välja högre säkerhet genom certifikatbaserad autentisering, eller autentisering med användarnamn och lösenord.

Programvaran kan installeras på alla Windows-versioner, 32 bitar och 64 bitar, från Windows 7 och framåt.

Förutsättningen för fullt fungerande programvara är förinstallation av .NET 2.0 (ingår i .NET 3.5.1)

Kommunikation sker på följande portar: 4321, 4322, 6251

Portarna är låsta och kan inte ändras.

NOX SIMS V6

SIMS är en Server/Client mjukvarulösning för multicentrala och grafiska lösningar med möjlighet till integration genom SQL Server. SIMS står för Security Information Management System.

Server:

Kommunikationen mellan SIMS Server och NOX-processorer är skyddad med en 384-bitars Blowfish-kryptering i alla Firmware-versioner upp till och inklusive version 9.85

Från R7 (version 10.0) används 256-bitars AES-kryptering och TLS 1.2 (SSL)

Från version 10.0 är det möjligt att välja högre säkerhet genom certifikatbaserad autentisering, eller autentisering med användarnamn och lösenord.

Programvaran kan installeras på alla Windows-versioner, 32 bitar och 64 bitar, från Windows 7 och framåt.

Förutsättningen för fullt fungerande programvara är förinstallation av .NET 2.0 (ingår i .NET 3.5.1) och .NET 4.5

Kommunikation sker på följande portar: 4322, 8777

Portarna är låsta och går inte att ändra, om det inte finns tillgång till port 8777 ska licensuppdateringar eventuellt utföras manuellt.

Klient:

Kommunikationen mellan SIMS Client och SIMS Server är skyddad med en 128 bitars AES-kryptering.

Programvaran kan installeras på alla Windows-versioner, 32 bitar och 64 bitar, från Windows 7 och framåt.

Förutsättningen för fullt fungerande programvara är förinstallation av .NET 2.0 (ingår i .NET 3.5.1) och .NET 4.5

Kommunikation sker endast med SIMS-servern på följande portar: 2010

Port 2010 rekommenderas men kan fritt ändras.

iNOX & NOX för Android, MacOS

iNOX och NOX för Android är smartphone-appar som kan komma åt NOX CPU via TCP/IP.

Kommunikationen är skyddad med en 384 bitars Blowfish-kryptering, i alla Firmware-versioner upp till och inklusive version 9.85

Från R7 (version 10.0) används 256-bitars AES-kryptering.

Från version 10.0 är det möjligt att välja högre säkerhet genom certifikatbaserad autentisering, eller autentisering med användarnamn och lösenord.

Kommunikation sker på följande portar: 4325

Porten rekommenderas men kan fritt ändras.

NOX SSH

NOX SSH är endast SSH Server, kommunikationen kan väljas att vara mellan 256 bitar till 4096 bitars Diffie Hellman, Private Key auth eller Public Key auth.

För ytterligare information, se Rebex webbplats, www.rebex.net, Rebex File Server -> Funktioner -> SSH Server

NOX PCIF (Allmänt skydd av PC gränssnitt)

Brute force prevention (Förhindra upprepade försök med fel kod över IP)

I R6 (<9.85x):

IP-gränssnittet följer det angivna antalet försök och tid, vilket väljs i NOX Config under "Allmänt -> Inställningar -> Användare -> Driftsblockering", när antalet försök har uppnåtts spärras IP-gränssnittet för den aktuella Source IP för det angivna antalet minuter (standardtid = 3 minuter).

I R7 (>10.0):

SL3: (Bakåtkompatibel status med endast kod)

IP-gränssnittet följer det angivna antalet försök och tid, vilket väljs i NOX Config under "Allmänt -> Inställningar -> Användare -> Driftsblockering", när antalet försök har uppnåtts spärras IP-gränssnittet för den aktuella Source IP för det angivna antalet minuter (standardtid = 3 minuter).

SL4: (Hög säkerhet, autentisering genom användarnamn och lösenord, TLS 1.2)

1. Det rekommenderas att använda lösenord med hög komplexitet. Kravet på komplexitet inställs i NOX Config under "Allmänt -> Inställningar -> Nätverksåtkomst/Nätverksnyckel -> Lösenordsregler"

2. För varje felaktigt inloggningsförsök sätts en fördröjning på 1 ms, denna ökas upp till 1 sekund, så det kommer att ta oproportionerligt lång tid att "gissa" koden. Denna fördröjning tas endast bort vid korrekt inloggning.

Kombinationen av komplexa koder och fördröjning anses vara ett särskilt säkert skydd mot brute force-försök.

NOX-kodpolicy (driftsenheter på NOX BUS)

Standardkonfigurationen blockerar alla kontrollpaneler i 3 minuter vid 5 felaktiga kodinmatningar, blockerar därefter alla paneler i 5 minuter vid inmatning av den 6:e felaktiga inmatningen. Det står beskrivet i Försäkring och Pensions (F&P) riktlinjer för AIA-anläggningar att det ska vara så här**.**
I NOX är det programmerbart, så vill man ha en striktare kodpolicy är det möjligt.

NOX-kort + PIN-kodpolicy (CMx-gränssnitt på NOX BUS)

Om PIN-koden anges felaktigt är standardinställningen att ingenting händer.
Det är en programmerbar funktion och är inte föremål för regler.

I praktiken innebär det att om du vill att ett kort ska spärras efter 3 felaktiga PIN-inmatningar så är det möjligt.

Ett spärrat kort kan därefter öppnas av en person som kan redigera användare via PC Control.

Dataflöde/bandbreddsförbrukning

SIMS Server -> SIMS Client

Kommunikationen mellan SIMS Server och SIMS Client består av krypterade data, mestadels händelser (text), den kräver nästan ingen bandbredd.

Det krävs mer när man ansluter en SIMS-klient till SIMS-servern för första gången, eftersom planlösningar överförs. Dessa ritningar cache lagras på klienten och synkroniseras på en ny anslutning om ändringar har skett.

Varje gång det sker en händelse i NOX-systemet skickas detta till SIMS-servern, varifrån det vidarebefordras till aktiva klienter. Varje evenemang består av max. 1 kB data, en händelse är en länk, larm, rörelse osv.

Den rekommenderade bandbredden mellan SIMS Server och SIMS Client är 2 Mbit/s, vilket kommer att täcka de allra flesta fall, då det motsvarar 256 händelser per sekund. För större SIMS-installationer med >50 NOX-processorer kan en högre bandbredd vara nödvändig.

NOX CPU -> SIMS Server

Kommunikationen mellan NOX CPU och SIMS Server består av krypterade data, mestadels händelser (text), den kräver lite bandbredd.

Varje gång det finns en händelse i NOX-systemet skickas detta till SIMS-servern. Varje event består av max. 1 kB data, en händelse är en länk, larm, rörelse osv.

Den rekommenderade bandbredden mellan NOX CPU och SIMS Server är 0,5 Mbit/s, vilket kommer att täcka de allra flesta fall då det motsvarar 64 händelser per sekund.

NOX CPU -> NOX Config/NOX PC Control

Kommunikationen mellan NOX CPU och NOX Config/NOX PC Control består av krypterade data, mestadels händelser (text), den kräver lite bandbredd.

Varje gång det finns en händelse i NOX-systemet skickas detta till aktiva kunder. Varje event består av max. 1 kB data, en händelse är en länk, larm, rörelse osv.

Den rekommenderade bandbredden mellan NOX CPU och SIMS Server är 0,5 Mbit/s, vilket kommer att täcka de allra flesta fall då det motsvarar 64 händelser per sekund.

Extern Applikation -> NOX

Det finns många typer av inkommande anslutningsalternativ för NOX, vad de har gemensamt är att de vanligtvis är textbaserade, därför kräver de nästan ingen bandbredd. Vissa av dessa alternativ erbjuder även kryptering (SSH/SDK). Eftersom det är varierande vad du vill skicka till NOX blir det nödvändigt att göra en bedömning från fall till fall. Vår erfarenhet är dock att 2 Mbit/s räcker i 99 av 100 fall.

NIS2 med NOX och SIMS

EU har skärpt kraven på företag och myndigheter inom området cyber- och informationssäkerhet, samtidigt har EU utökat omfattningen av vilka typer av företag som kommer att beröras i framtiden.

NIS2 (Network and Information Systems version 2) riktar sig till elektroniska kommunikationsnätverk, enheter som bearbetar digitala data eller system som lagrar data.

NOX

NOX är ett certifierat och godkänt system enligt EN50131 klass 3, den högsta säkerhetsklassen i EU för inbrottslarmsystem.

I samband med installation av NOX i ett företag är det kritiskt att säkra kommunikationen med centralenheten, eftersom centralenheten är den enda nätverksanslutna enheten i ett NOX-system. Som det framgår av detta dokument är all nätverkskommunikation krypterad, och därför kommer NOX att kunna ingå som en säker enhet i en eventuell NIS2 bedömning.

Alla inbrottslarm- och passersystemskomponenter är anslutna till en RS-485-BUSS som är säkrad med en egenutvecklad algoritm uppfunnen av NOX Systems.

SIMS

Om ett företag vill använda SIMS (Multi Central Management platform till NOX) gäller samma princip som ovan. Det är kritiskt att säkra kommunikationen mellan SIMS och centralenheten, eftersom centralenheten är den enda nätverksanslutna enheten i ett NOX-system.

SIMS är en Windows-baserad applikation som kommer att installeras på en server och kan ingå i kundens IT-miljö, med gällande patch- och underhållsplaner på lika villkor med andra IT-system.

Allmänna rekommendationer

Det rekommenderas att endast använda nätverkstekniker som stöder krypterad kommunikation, de enskilda nätverksteknikerna beskrivs i detalj i detta dokument.

I samband med etableringen av kortläsare rekommenderar vi att använda krypterad OSDP-kommunikation för läsare, i kombination med DESFire EV2/EV3 och Secure File Reading som kortteknologi. På så vis uppnås största möjliga säkerhet på kort och läsare, vilket samtidigt hindrar kopiering av kort och Ev. "man-in-the-middle-attacks".

Alla NOX-komponenter som ingår i en certifierad installation ska hålla en säkerhetsnivå som motsvarar kundens eller eventuellt tredjeparts krav.

Om det finns behov av ytterligare stöd gällande detta, eller behov av en icke-bindande diskussion om säkerheten i ett NOX-system, är du välkommen att kontakta oss.

Principritning av en NOX- och SIMS-installation