JANUARY 23, 2024

PROTECTING NETWORK RESILIENCY

NETWORK RESILIENCE COALITION (NRC)

CENTER FOR
CYBERSECURITY
POLICY AND LAW

Contents

Abstract

This whitepaper is a publication of the Network Resilience Coalition (NRC), a cross-industry collaborative effort run by the Center for Cybersecurity Policy and Law (CCPL). This document is intended for a broad audience of cybersecurity decision-makers and implementers at network product vendors and the consumers that use them, particularly in telecommunications and network infrastructure. The recommendations given are at a high level and are intended to guide strategic and tactical decision-making within the networking cybersecurity ecosystem, and hopefully to provide a framework to enhance discussions with relevant public sector stakeholders.

Vulnerabilities, flaws, or misconfigurations in network device software, firmware, and hardware can have a devastating effect on network providers and their downstream consumers. What makes addressing these challenges particularly difficult in the network provider space? As a community not just of providers but also of network product vendors, what could we be doing better? In this paper, the coalition discusses this problem and these questions, then proposes a set of best practices for the industry as a whole and provides input to policymakers on how regulatory bodies can positively impact the ecosystem.

About Us

The Network Resilience Coalition

The Network Resilience Coalition (NRC) was founded in mid-2023 with a vision to improve the security, safety, and resilience of the hardware and software that make up our networks. Members consist of companies that are either vendors of networking hardware and software, or consumers and deployers of those products. Together, these members are working toward a shared goal of uplifting the entire ecosystem through technological innovation, collaborative standard and best-practice setting, and acting as a resource for policymakers in the space. The NRC operates under the Center for Cybersecurity Policy and Law alongside similarly collaborative efforts.

The Center for Cybersecurity Policy and Law

The Center for Cybersecurity Policy and Law is an independent organization dedicated to enhancing cybersecurity worldwide by providing government, private industry, and civil society with practices and policies to better manage security threats. Established in 2017 as a 501(c)(6) nonprofit within Venable LLP's Cybersecurity Services group, the Center combines policy expertise with convening power to bring industry leaders together with policymakers, form coalitions, and launch initiatives that produce real-world outcomes.

Executive Summary

Networking infrastructure, and the software and hardware that it consists of, is critical infrastructure of the utmost importance. Failing to protect these systems carries not only a heightened business risk but also a risk to the technologies that our entire society relies on to function. Today, misconfigured or end-of-life products represent a massive attack surface for adversaries, and communication gaps between product vendors and consumers add additional challenges.

To that end, the Network Resilience Coalition makes several recommendations on best practices for both vendors and users of network products. The Coalition believes that any potential additional costs incurred by these practices are outweighed by the downstream mitigation of disruptive or damaging incidents and further justified by the broad impact of increasing network resilience across the board.

The NRC recommends that vendors of network products:

- Align their software development practices with the NIST Secure Software Development Framework (SSDF)

- Provide clear and concise details on product "end-of-life" by providing specific dates, date ranges, and details on what level of support to expect for each date range
- Avoid combining critical security fixes from updates with new features or functionality enhancements
- Consider participation in the OpenEoX effort in OASIS, a cross-industry effort to standardize the way end-of-life information is communicated and to provide it in a machine-readable format.

The NRC recommends that consumers and purchasers of network products:

- Align their product procurement requirements with the above recommendations by favoring vendors that are aligned with the SSDF, that provide clear end-of-life information, and that plan to provide separate critical security fixes
- Increase cybersecurity vigilance (vulnerability scanning, configuration management) on products they elect to rely upon outside of their support period
- Periodically ensure that product configuration is aligned with vendor recommendations, with increasing frequency as products age
- Consider participation in the OpenEoX effort in OASIS, a cross-industry effort to standardize the way end-of-life information is communicated and to provide it in a machine-readable format.

Coalition members, both vendors and consumers, agree that these recommendations, if broadly implemented, would lead to a more secure and resilient global network infrastructure. It is the opinion of the group that this is mutually beneficial to all participants of the network product market, and that it also makes major strides in better protecting the critical infrastructure that people rely on for their livelihoods and well-being.

Introduction

Networks around the globe are made up of an intricate and complex web of hardware and software, all carefully configured and managed to keep vital communications operational twenty-four hours a day, seven days a week. Any disruptions could have catastrophic downstream impacts, causing significant material damage to global business or even endangering human lives. It is imperative to take great care to protect network hardware and software from malicious action, unintentional flaws, or just degradation over time.

Vendors of these products will provide support for some predetermined period — software updates, firmware fixes, technical assistance, etc. — or they will recommend that the provider purchase something new if the software or hardware in question is too old or "out of support." Ideally, the provider would use the purchased product or service for the safe lifetime as defined by the vendor, then replace it. And ideally, the vendor would ensure that any issues or vulnerabilities are promptly fixed before there are damaging consequences.

These ideal cases don't often happen in today's world. It is the NRC's opinion that this is not to place blame on any individual actor or on either side of the supply chain, but rather the reality of using still-functional networking products where weaknesses may be discovered beyond their supported lifetime. We intend to provide our unique combined insight on what these weaknesses are, why they have been so difficult to overcome in the past, and most important, what we think can be done to make a more resilient ecosystem.

A Global and Cross-Industry Issue

Taken as a general issue, addressing the issues caused by vulnerabilities or flaws is part of a wider technology sector supply chain and lifecycle management discussion. It stretches across all industries, although each has slight differences that warrant particular focus from working groups and consortiums. As each group works to engineer solutions to its specific slice of the problem, there is often an implicit reliance on network infrastructure operating correctly and securely. The core components of our networks are often treated as a

given, but as bad actors pay more attention to these core aspects because of their relevance to critical infrastructure and internet-of-things applications, the importance of improving the overall resilience of our networks is clear.

Problem Statement

While difficulties remain in addressing flaws and vulnerabilities in general, there are unique difficulties in handling the issue when it applies to products that make up network infrastructure. We scope the problem statement to these specific challenges and highlight the following as the most relevant:

1. Networking products cannot be supported indefinitely for economic reasons; as the ecosystem continues to advance, updates to old products become progressively more expensive to produce and more difficult to deploy.

2. Networking product deployments, often in remote locations or in bespoke environments, are challenging for operators to seamlessly update or replace.

But vulnerabilities are frequently discovered in the above products, and a wholesale replacement with a newer product may be equally infeasible for the user. Establishing a shared understanding of technical best practices and the expectations of vendors and users is the most effective path forward to mitigate the problem.

Understanding the Problem

There is an inclination for the severity of the problem to be trivialized or minimized by those who don't understand the full complexity involved. Part of the goal of the NRC is to allow the multiple parties involved in network infrastructure to learn more about each other's processes and challenges.

End-of-Life Products

While it is important to recognize that a strict division between vendors of network products and users of network products is neither helpful nor particularly realistic, understanding the viewpoints of each side of the supply chain helps provide a better overall picture of the problem.

From a network product vendor perspective, providing post-purchase support for a product has a material and opportunity cost and can be technically difficult. Catching flaws or vulnerabilities is an imperfect science, and even the most secure-by-design products end up with issues that need to be fixed after release. Additionally, finding, and particularly fixing, these issues takes engineering time and resources. Supporting a product indefinitely is economically infeasible, and as technology shifts and the ecosystem evolves, a product can become so out-of-date that even updating it becomes impossible. Vendors want their products to be as safe and as secure as possible and spend significant resources on that goal, even when it no longer provides any additional profit.

From a network product user perspective, ongoing support is an important part of continuing to use a product, but this issue often is not raised until support ceases at the time the product enters end-of-life. It is an unfortunate reality that insufficient attention is paid at the time of acquisition to end-of-life plans for that technology.

Challenging Deployment Circumstances

Deployments of networking products tend to be in large, complex, interconnected technology stacks with bespoke and intricate components. Add to this the common physical obstacles of product deployment — atop towers, buried underground, or sparsely spread across large enterprises — and the problem begins to become clear.

Each of these challenges raises the average cost of maintaining network products through updates, upgrades, and fixes. In the case of complex technology stacks, a software update that fixes a critical security flaw may also make an unrelated change that renders the software incompatible with the rest of the solution. The deployer must spend significant time and resources performing thorough testing before any true changes are made. The risk level is high, and downtime must be minimized for downstream customers.

Remainder of the Problem Space

Even outside the two specific classes of products and their challenges described above, network software and hardware will have vulnerabilities go unpatched and subsequently be exploited, or may have unmitigated flaws that cause incidents. These more traditional problems are also addressed by more traditional mitigating solutions and are therefore not the focus of this paper. Other groups and efforts are attempting to address the supply chain and lifecycle management processes, and their progress is likely to translate without issue to address the same problems in this specific domain of network resilience.

The Cloud and Virtual Networks – Not an Instant Solution

Offloading management of devices to a cloud service, utilizing virtualized or software defined networks, and other similar approaches seem to offer a solution to many of the problems discussed above. But virtualized networks and cloud services still must use real hardware and software to operate their networks. The safety and security of the "real" network directly correlate to the safety of using a virtualized system.

Addressing the Problem – Recommendations

Below we provide guidance on how both coalition members and the ecosystem at large can begin to tackle this issue. These are concrete and discrete action items, some of which are already being implemented at various organizations. The Coalition hopes to reinforce the importance of those activities where they are already being done, and to encourage the industry to take steps toward accomplishing the tasks where there are implementation gaps.

Recommendations for Product Vendors

1) Create Secure-by-Design Products and Configurations

a) Vendors should follow secure-by-design practices for software, hardware, and firmware products. Where possible, these practices should be aligned to industry best practices, such as those defined in the NIST Secure Software Development Framework (SSDF).

b) Initial or recommended configurations for products should strive to be secure-by-default.

2) Provide Clarity on End-of-Life

a) Products should have firmly defined end-of-life (EOL) dates and details. If there are multiple phases of EOL, each should have clear dates and details.

b) If possible, provide EOL details publicly and in a static, web-addressable location.

c) Any deviations from the standard details in a particular contract should be clearly stated in that contract.

d) Where possible, utilize standardized and/or machine-readable language to specify the conditions and details of the end-of-life, such as by using OpenEoX.

3) Create and Distribute Patches Mindfully

a) Updates or patches should not adjust or reset configuration unless it is relevant to fixing or addressing a vulnerability or flaw.

b) Where possible, distribute high-criticality security fixes separate from feature updates, such that the security patch can be applied quickly without disrupting operation. Dedicated security fixes without other additions allow for faster response times and significantly easier testing.
c) Patches that fix critical issues should not make breaking changes to a product or its APIs.

4) Get Involved and Contribute to the Dialogue

a) Get involved in or remain up to date on industry standardization efforts, such as OpenEoX in OASIS.
b) Nurture an open and two-way channel of cooperation between yourself and product users.
c) Regardless of involvement level, be willing to share information, lessons learned, and technical feedback to industry community groups, if possible.

Recommendations for Product Users and Maintainers

1) Procure Products that Align with Best Practices and Above Recommendations

a) Favor vendors that adhere to the above recommendations during procurements.
b) Encourage vendors to align with security best practices by providing them as requirements in Requests for Proposals or in service contracts.

2) Increase Cybersecurity Vigilance on End-of-Life and End-of-Support Products

a) While an upgrade is not feasible, intensify risk management and configuration management activities on products that have exited their period of primary vendor support.
b) Until such time as an unsupported product can be replaced, mitigating controls should continue to be implemented — particularly as these products get further outside of their support date ranges.

3) Implement and Maintain Vendor-Recommended Product Configuration

a) Use the vendor-recommended configurations where applicable and reaffirm that those configurations are correct on a risk level-appropriate basis.
b) When severe vulnerabilities are discovered, open a dialogue with the relevant vendor to bring the vulnerability to their attention and to learn of any current or potential patches or configuration guidance.
c) Monitor vendor security notifications to ensure awareness of new vulnerabilities and the need to upgrade.

4) Get Involved and Contribute to the Dialogue

a) Get involved in or remain up to date on industry standardization efforts, such as OpenEoX in OASIS.
b) Nurture an open and two-way channel of cooperation between yourself and product vendors.
c) Regardless of involvement level, be willing to share information, lessons learned, and technical feedback to industry community groups, if possible.
d) Provide support to technical experts to allow for their input and feedback to be provided to these groups, even if it is outside their typical duties.

Next Steps

The Network Resilience Coalition acknowledges the difficulty of solving these problems and the complexities that make a single solution infeasible. The recommendations provide organizations in the networking ecosystem a concrete set of steps that will improve not only their own security posture, but also the resilience of the vast, interconnected system we rely on.

Organization-level recommendations like the above can be difficult to act on as an individual. Regardless of the reader's associated organization or level of authority within that organization, the following personal steps can facilitate real and measurable progress toward a more secure and resilient future:

- Use this document to encourage good cybersecurity and network resilience practices to be followed at your organization, and as a reference for including requirements for the products and services you purchase.
- Get personally involved in the spaces where this collaborative work is being done. The NRC would particularly like to recommend engagement with the OpenEoX standardization effort.
- Contribute to the conversation with policymakers, encouraging them to understand the complexities of the problem and how they can help industry tackle these challenges.

As individuals, as companies and organizations, as vendors or consumers, we benefit from a more secure world. The Network Resilience Coalition thanks its members for their contributions and hard work toward realizing this future.

References and Links

Homepage of the OpenEoX Initiative:

https://openeox.org/

OASIS Technical Committee for OpenEoX:

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openeox

NIST Secure Software Development Framework (SSDF):

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf