Forescout Technologies, Inc.
Response to National Telecommunications and Information Administration (NTIA)
Software Bill of Materials Elements and Considerations
Request for Public Comment

Contact: Yejin Jang, Government Affairs Director
FORESCOUT TECHNOLOGIES, INC., 190 TASMAN DR., SAN JOSE, CA 95134
Yejin.jang@forescout.com

On behalf of Forescout Technologies, Inc. (Forescout), thank you for the opportunity to provide a comment on the National Telecommunications and Information Administration's (NTIA) Notice and request for public comment on *Software Bill of Materials Elements and Considerations* (Notice).

Introduction: Forescout Technologies, Inc. and Forescout Research Labs

Forescout Technologies, Inc. is a cybersecurity company based in San Jose, California and is the market leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environment and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous security posture assessment.

Forescout's market leadership is reinforced by Forescout Research Labs, a mission-driven team that develops technology and insights to help protect connected communities. With the benefit of Forescout Device Cloud, the world's largest crowd-sourced device knowledgebase with over 12 million device fingerprints, our research team continuously finds new ways to help ensure we are delivering the world's best cybersecurity for any kind of networked device. The Forescout Research Labs team monitors the global threat landscape and is constantly creating new tools and techniques to identify, understand and manage the threats and risks associated with our ever-expanding device ecosystem.

Forescout research shows the need for increased transparency in supply chain security

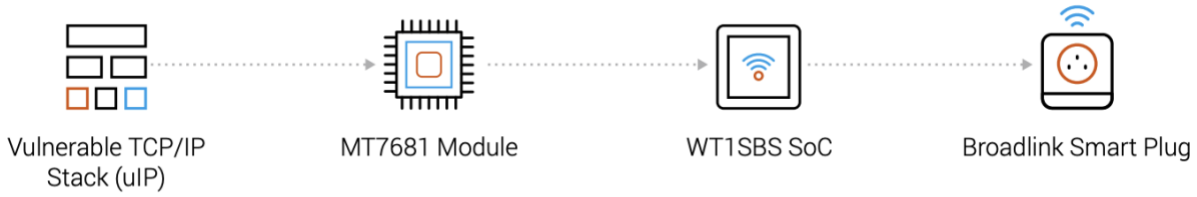
In June 2020, JSOF publicly released a set of 19 vulnerabilities, collectively called Ripple20, which affected the Treck embedded TCP/IP stack. Forescout Research Labs partnered with JSOF using data from Forescout's device cloud to identify potentially affected devices and vendors. Treck is a basic connectivity component used by a range of device vendors in many different ways. For instance, the stack can be used with or without a real-time operating system, is highly configurable and is licensed under different names (for instance, Elmic commercializes the stack for the Asian market using the name KASAGO). Vendors usually do not advertise that they use this particular TCP/IP stack, just as they rarely advertise the many software and hardware components that go into their devices. Essentially, in the IoT world, there is no public bill of materials that allow users and organizations to know the components that are part of the devices they use. Most of the issues in Ripple20 relate to the implementation of the TCP/IP stack, which means they do not depend on specific applications, and the adversary only needs network access to the targeted device to leverage the vulnerabilities and take control of the device.

Building on the security value of Ripple20 , Forescout Research Labs launched Project Memoria with the mission of providing the cybersecurity community with the largest study on the security of TCP/IP stacks. To date, Forescout has released three reports: AMNESIA:33, NUMBER:JACK, and NAME:WRECK, which focus on analyzing vulnerabilities in TCP/IP stacks commonly found in embedded devices.

AMNESIA:33 was published on December 8, 2020. AMNESIA:33 is a set of 33 new memory corruption vulnerabilities impacting millions of IoT, OT and IT devices that present an immediate risk for organizations worldwide.

Report Highlights:

- AMNESIA:33 affects multiple open-source TCP/IP stacks that are not owned by a single company.
- The long and fuzzy nature of the supply chain may not be evident at first glance. For example, a Broadlink Smart Plug uses a system-on-a-chip (SoC), which contains the popular MediaTek MT7681 Wi-Fi module, which leverages the vulnerable uIP stack. Hence, it may not be evident that the Broadlink Smart Plug is vulnerable to AMNESIA:33 and requires patching.



Supply chain example, the Broadlink Smart Plug

- Following the point above, device vendors may take months to issue patches due to the difficulty in identifying end products using affected components. For example, B&R automation released an advisory mentioning more than 100 vulnerable product models in May 2021, more than 5 months after the initial disclosure of AMNESIA:33. As mentioned in their advisory: *"One B&R POWERLINK stack includes a proprietary TCP/IP stack which is related to a TCP/IP stack affected by Amnesia."*

NUMBER:JACK was published on February 10, 2021. It disclosed nine vulnerabilities in multiple TCP/IP stacks that improperly generate ISNs (Initial Sequence Numbers) within TCP connections, leaving a device's TCP connections open to attacks.

Report Highlights:

- Although NUMBER:JACK vulnerabilities are not as critical as those of AMNESIA:33, they are even more prevalent, affecting 9 of 11 stacks analyzed.
- Weak ISN generation is one more instance of historical vulnerabilities discovered and fixed in the IT world decades ago that today affects large numbers of IoT and OT devices.

NAME: WRECK was a collaborative study published by Forescout Research Labs and JSOF on April 13, 2021. It discloses nine DNS-based vulnerabilities affecting four popular TCP/IP stacks

used in millions of IoT, OT and IT devices, and allows for Denial of Service or Remote Code Execution.

Report Highlights:

- The affected stacks have been used for decades in several critical OT and embedded devices, as well as IT servers and network appliances.
- One of the vulnerabilities in NAME:WRECK, affecting the IPnet TCP/IP stack was rediscovered independently. This vulnerability was originally reported by other researchers to Wind River in 2016 but never assigned a CVE, which means that many other products using that stack as a component were not secured at the time.
- It is noteworthy that when a stack has a vulnerable DNS client, there are often several vulnerabilities together, including potential RCEs.

The TCP/IP stacks Forescout analyzed show there is great need for transparency in software development. It also shows that the development environment is complex; even when the same software component is used, it may be called different things and may impact a variety of devices. Adding to the complexity, device and component vendors may be unaware of the full list of device models and products lines that are impacted. Further, even where an SBOM exists, it may be outdated, not reflect updates, or otherwise inaccurate which creates additional supply chain challenges.

Additional use case considerations for SBOM connected to network observables
The data fields enumerated in the Notice (supplier name, component name, component version, cryptograph hash, unique identifiers, dependency relationship, SBOM author) are, as described, minimum elements which will be useful in driving SBOM adoption and implementation. When minimum elements articulated in an SBOM are correlated with network observables, the combined force of these data provide greater value for risk mitigation.

Network observables, or a string that can be observed on the network that indicates the presence of certain components (e.g., application-layer banners), can be used for network monitoring solutions to verify the presence of components on networked devices and to verify whether a device has been modified (e.g., a patch has/has not been applied). When SBOM minimum elements are combined with information from network observables, organizations would be able to see whether a device or component has accessed something outside of an enumerated spec which could indicate compromise. Additionally, network observables can also be used for automatic generation of, at least partial, SBOMs for older devices that are no longer supported.

Additional data field element for SBOM
A "security contact" data field may also be beneficial in mitigating risk. This could be an email from the Product Safety and Incident Response Team (PSIRT) for a vendor who can be contacted for vulnerability disclosures. This can also be used by security researchers that find vulnerabilities to understand what devices are affected. An example of this concept is provided at https://securitytxt.org/.

Question to consider - technological methods for enriching and validating SBOMs

When there is a knowledge gap in what devices or software are impacted, NTIA may want to consider whether additional technological methods to either enrich or validate SBOMs exist and the value of said enrichment or validation in mitigating supply chain vulnerabilities. Further, would such a function also help in instances where an SBOM does not exist?

Forescout concur with NTIA's assessment and support for automated SBOMs
As stated in the Notice, automated SBOM generation must be supported for SBOM to scale. Forescout concurs with this assessment and would note that for an organization of our size, manual generation of SBOM would be untenable given the variety of products that are offered.

SBOMs do not obviate the need for fundamental cybersecurity protections
Discussion about SBOM adoption and implementation is encouraging but has yet to reach full scale adoption. In the interim, organizations should focus on implementing a zero trust architecture (ZTA) that assumes compromise and access requests to information resources are dynamically evaluated and only granted when the request meets organizational trust policies. ZTA is described in NIST Special Publication 800-207: Zero Trust Architecture.

Additionally, organizations may want to consider implementing an information security continuous monitoring (ISCM) program which can provide "visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls."[1] ISCM is described in NIST Publication 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations.

[1] Kelly Dempsey et al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations, Abstract, September 2011.