Network Visibility Security Advisory Policy

Revised June 2024, Rev C

Preface

The following guidelines will be used as a basis for decisions regarding vulnerability responses concerning Keysight Network Visibility Systems ("NVS") products. NVS products include such items as network packet brokers, active taps, and bypass switches. It should be noted that these products are not typically Internet facing and should not be evaluated using the same criteria as web servers and the like. Additionally, while many of our products have operating systems that are based partially or entirely on commercial operating systems, they often have limited user access which also needs to be considered when evaluating exploitability of vulnerabilities.

The following policies will govern decisions, but Keysight will evaluate each vulnerability and product susceptibility independently and assess impact relative to the market and our customers. Keysight reserves the right to make decisions based on the circumstances of each unique vulnerability instance.

Vulnerability Inquiries

Vulnerability inquiries should be submitted through the standard Keysight Support channels – support@keysight.com. Feedback to Keysight responses can be escalated to vulnerability@ixiacom.com.

Vulnerability Testing

Vulnerability testing of each software release is performed multiple times during each release cycle using at least two different commercial security scan tools. Vulnerabilities discovered during the release cycle are resolved within the release process whenever possible, and critical or high severity vulnerabilities receive the highest level of Engineering attention. That approval may be given due to a false-positive from the scan tools, a lack of exploitability of the vulnerability, or a low-impact published mitigation. Earlier releases are not re-scanned as a matter of process, though new vulnerabilities flagged during a release cycle are evaluated for their impact to the most recent published builds. Vulnerabilities reported from the field during a release cycle are subject to the same treatment as vulnerabilities detected by internal scans.

Keysight is committed to meeting current and future US, European, and other applicable software security requirements and will continue to revise this policy, in its sole discretion, in accordance with regulatory guidelines.

KEYSIGHT

Vulnerability Response SLA

Keysight's response to customers will be based upon the NIST CVSS base score of the vulnerability. Exposure communications will include a description of the exploitability of the vulnerability and any mitigation procedure or work-around as well as an ETA on the next communication detailing the delivery of a fix. The following SLA will be maintained:

Vulnerability Severity	SLA
High NIST CVSS score of 7.0 – 10.	Keysight will provide a response regarding vulnerabilities of a HIGH severity within 2 business days.
Medium NIST CVSS score of 4.0 – 6.9.	Keysight will provide a response regarding vulnerabilities of a MEDIUM severity within 5 business days.
Low NIST CVSS score of 0 – 3.9.	Keysight will provide a response regarding vulnerabilities of a LOW severity within 10 business days.

Vulnerability Resolution SLA

Keysight's resolution to customers will depend on the severity of the vulnerability and the complexity of the resolution itself. Keysight will follow these guidelines:

Vulnerability Severity	Guideline
High NIST CVSS score of 7.0 – 10.	Keysight will provide a response regarding the resolution of HIGH severity vulnerabilities within 5 business days of the determination that a product is susceptible to that vulnerability. The resolution itself will be made available as soon as possible.
Medium NIST CVSS score of 4.0 – 6.9.	Keysight will provide a response regarding the resolution of MEDIUM severity vulnerabilities within 10 business days of the determination that a product is susceptible to that vulnerability. The resolution itself will be targeted for inclusion in the next scheduled release.
Low NIST CVSS score of 0 – 3.9.	Keysight will provide a response regarding the resolution of LOW severity vulnerabilities within 20 business days of the determination that a product is susceptible to that vulnerability. Keysight will assess the need for a fix resolution based on its assessed risk to its customers

Vulnerability Summary

The following table summarizes expected response times for vulnerability questions raised by its customers.

Tasks	Business Day Response
Support opens Case	Same day response (t-0)
Support Keysight's CVE database & responds to customer	Same day response
If fix is available Support provides to customer	Same day response
Else, Support escalates to Engineering for assessment	Same day response
Sev HIGH Exposure Comm., mitigations, ETA for Plan	T + 2
Sev HIGH Resolution Plan	< t + 7
Sev HIGH Resolution Delivery	ASAP Patch delivery
Sev MEDIUM Exposure Comm., mitigations, ETA for Plan	T + 5
Sev MEDIUM Resolution Plan	< t + 15
Sev MEDIUM Resolution Delivery	Target next schedule release
Sev LOW Exposure Comm., mitigations, ETA for Plan	< t + 10
Sev LOW Resolution Plan	< t +30
Sev LOW Resolution Delivery	Scheduled as needed

Vulnerability Resolution Delivery

Keysight recognizes that in controlled environments it is often easier to absorb a strategic patch release over a full release. While sensitive to customer acceptance test procedures, Keysight will weigh the nature of the fix with the current release environment to select the best possible delivery mechanism.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2018 – 2024, Published in USA, June, 2024.