Vulnerability Disclosure Program Policy (VDPP) and Rules of Engagement (ROE) for Nextivity, Inc. (“Nextivity”)

Version 1.0
May 22, 2023

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	May 22, 2023	Initial draft

Contents

1. PURPOSE

This policy provides security researchers with clear guidelines for (1) conducting vulnerability and attack vector discovery activities directed at certain Nextivity, Inc. equipment and (2) submitting those discovered vulnerabilities. This policy has been developed in consultation with AT&T and other security researchers.

2. OVERVIEW

Nextivity technologies are deployed in critical infrastructure systems and first responder missions. The proper functioning of these systems and applications can have a significant impact in assisting agencies, enterprises and other organizations in accomplishing their mission critical communications.

Maintaining the security of our equipment either in stand-alone or broader networks is a high priority at Nextivity. Ultimately, our work ensures that we can assist organizations in accomplishing their missions and contribute to the success of the individuals associated with those organizations.

Nextivity recognizes that researchers regularly contribute to the work of securing our communications devices, infrastructure and the Internet as a whole. Therefore, Nextivity invites reports of any vulnerabilities discovered on the MegaFi product, its applications, and its cloud service. Information submitted to Nextivity under this policy will be used for defensive purposes, which is to say, in mitigating or remediating vulnerabilities in our equipment or networks.

Hereinafter, researcher[1] may be referred to as “you” or “your” and Nextivity may be interchangeably used in conjunction with or alternatively referenced as “we”, “our”, or “us”.

3. SCOPE

This policy applies to the AW12 and MegaFi products, their application in networks, and related web-based cloud services utilized in the management of these Nextivity products. All other equipment, systems or other services not specifically listed above are not included within the scope of this policy.

[1] The term “Researcher” in this document is intended to be consistent with the terms “Finder” and/or “Reporter” as used in ISO/IEC 29147:2014(E) and the CERT® Guide to Coordinated Vulnerability Disclosure, and may be substituted with “you, your”.

4. HOW TO SUBMIT A REPORT

Please submit a report of the vulnerability at https://nextivityinc.com/products/shield-aw12-hpue. An example of the vulnerability report would include a detailed summary, including:

- Type of vulnerability
- IP Address or hostname
- Description of vulnerability
- Instructions to replicate vulnerability
- Potential impact to system/site
- Recommended remediation actions

5. GUIDELINES

You MUST read and agree to abide by the guidelines in this policy for conducting security research and disclosure of vulnerabilities or indicators of vulnerabilities related to products, services, and systems listed above. We will presume you are acting in good faith when you discover, test, and submit reports of vulnerabilities[2] or indicators of vulnerabilities in accordance with these guidelines:

- You MAY[3] test Nextivity's products, services, and internet-accessible systems to detect a vulnerability or identify an indicator related to a vulnerability for the sole purpose of providing Nextivity information about such vulnerability.
- You MUST avoid harm to Nextivity products, services, systems and operations.
- You MUST NOT exploit any vulnerability beyond the minimal amount of testing required to prove that the vulnerability exists or to identify an indicator related to that vulnerability.
- You MUST NOT intentionally access the content of any communications, data, or information transiting or stored on Nextivity products or information system(s) – except to the extent that the information is directly related to a vulnerability, and the access is necessary to prove that the vulnerability exists.

[2] Vulnerabilities throughout this policy may be considered "security vulnerabilities" as defined by Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, § 102 "The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control."

[3] The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 which can be found at https://www.ietf.org/rfc/rfc2119.txt.

- You MUST NOT exfiltrate any data under any circumstances.
- You MUST NOT intentionally compromise the privacy or safety of Nextivity personnel or any legitimate third parties.
- You MUST NOT intentionally compromise the intellectual property or other commercial or financial interests of Nextivity or any of its personnel or entities or any legitimate third parties.
- You MUST NOT disclose any details of any extant Nextivity products, service, or system vulnerability or indicator of vulnerability to any party not already aware at the time the report is submitted to Nextivity.
- You MAY disclose to the public the prior existence of vulnerabilities already fixed by Nextivity, potentially including details of the vulnerability, indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability. If you choose to disclose, you should do so in consultation with Nextivity.
- You MUST NOT disclose any incidental proprietary data revealed during testing or the content of information rendered available by the vulnerability to any party not already aware at the time the report is submitted to Nextivity.
- You MUST NOT cause a denial of any legitimate services in the course of your testing.
- You SHOULD strive to submit high-quality reports.
- You MUST NOT submit a high-volume of low-quality reports.
- You MUST comply with all applicable Federal, State, and local laws in connection with security research activities or other participation in this vulnerability disclosure program.

If at any point you are uncertain of whether to proceed with testing, please contact our team at support@nextivityinc.com.

6. PARTICIPANT EXPECTATIONS

We take every disclosure seriously, and very much appreciate your efforts. We are committed to coordinating with you as openly and expeditiously as possible. The contents of information provided in the reports and follow-up communications are processed and stored on a Nextivity information system within the United States. You can expect us to do the following:

- We SHALL investigate every properly reported vulnerability and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.
- If you opt to provide your contact information, our security team MAY contact you for further information.

- We SHALL, to the best of our ability, validate the existence of the vulnerability.
- We MAY disclose to the public the prior existence of vulnerabilities remedied by us, potentially including details of the vulnerability such as the indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability.
- In the event that we choose to publicly disclose your reported vulnerability we SHALL recognize your contribution as it must pertain to improving our security, the first to report a unique vulnerability, and if your report triggers a code or configuration change.
- In the event you report a vulnerability pertaining to a component of our product provided by others, we SHALL validate the vulnerability pertaining to the component product. If it is determined as a component vulnerability, we MAY report the product vulnerability to the affected vendor or to a third-party vulnerability coordination service.
- We SHALL NOT forward your name and contact information to any affected component vendors unless otherwise requested by you.
- We MAY NOT disclose information provided by any vendor unless the vendor explicitly states to do so.
- We SHALL request 30 days for acknowledgement and 180 days for mitigation development, and deployment.
- We MAY consult with you and any affected vendors to determine our public disclosure[4] plans of the vulnerability.
- In cases where a product is affected and the component vendor is unresponsive, or fails to establish a reasonable timeframe for remediation, we MAY disclose product vulnerabilities 45 days after the initial contact is made, regardless of the existence or availability of patches or workarounds from affected vendors.

[4] "Public disclosure" means the release of previously undisclosed information related to a vulnerability by Nextivity, a component vendor, or a researcher to or through mediums that include, but are not limited to, official press releases, blogs, social media platforms, email, or other webpages. We SHALL make our disclosure determinations based on relevant factors, such as: whether the vulnerability has already been publicly disclosed, the severity of the vulnerability, potential impact to critical infrastructure, possible threat to public health and safety, immediate mitigations available, component vendor responsiveness and feasibility for creating an upgrade or patch, and vendor estimate of time required for customers to obtain, test, and apply the patch. Active exploitation, threats of an especially serious nature, or situations that require changes to an established standard may result in earlier or later disclosure.

7. LEGAL / AUTHORIZATION

If you make a good faith effort to conduct your research and disclose vulnerabilities in accordance with the guidelines set forth in this policy, (1) Nextivity will not recommend or pursue any law enforcement or civil lawsuits related to such activities, and (2) in the event of any law enforcement or civil action brought by any entity other than Nextivity, Nextivity will affirm that your research and disclosure activities were conducted pursuant to, and in compliance with, this policy. This agreement is effective at the time of the form submission on the Nextivityinc.com webpage.

Please note that individuals and entities that conduct activities as authorized by this policy and comply with its terms will receive legal protection from criminal or civil liability under section 1030 of title 18, United States Code, and similar laws penalizing unauthorized access to computers.

Nextivity does not authorize, permit, or otherwise allow (expressly or implicitly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this policy or the law. Any activities that are inconsistent with this policy or the law may lead to criminal and/or civil liabilities. Third parties (e.g., any non-Nextivity entity) may independently determine whether to pursue legal recourse or related activities.

Nextivity may modify the terms of this policy or suspend this policy at any time.