MTN Group

https://www.mtn.com/

Reports resolved

4258

Assets in scope

376

Submit report

Vulnerability Disclosure Program

Launched on Dec 2019

★ 🔔

Bookmarked Subscribed

Policy Scope New! Hacktivity Thanks Updates (0)

Policy

At MTN, we are committed to keeping our systems, network and product(s) secure. Despite the measures we take, the presence of vulnerabilities will always be possible. When such vulnerabilities are found, we'd like to learn of them as soon as possible, allowing us to take swift action to improve our security.

MTN's approach to Responsible Disclosure is as follows, you are allowed to search for vulnerabilities, as long as you don't:

• Execute or attempt to execute a Denial of Service (DoS)
• Make changes to a system
• Install malware of any kind
• Social engineer our personnel or customers (including phishing)
• Scan or run tests in a manner that would degrade the operation of the service or negatively affect our customers in any way
• Physically attack or damage MTN property, offices or data centres or attempt to do so
• Run tests on third party applications, websites or services that integrate with or link to MTN
• Scan or attack any cloud hosted infrastructures such as Azure or Amazon Web Services or attempt to do so
• Make use of any kind of automated scanning software.

Breaching the above restrictions may result in MTN launching an investigation and/or taking legal action to the greatest extent of MTN's legal obligation and rights or that of our partners and customers.

What we ask of you:

• Do not abuse or exploit discovered vulnerabilities in any way for any purpose
• Do not share discovered vulnerabilities with any entities or persons other than MTN and its employees until after MTN has confirmed the vulnerability has been resolved
• Provide us with adequate information to enable us to investigate the vulnerability properly. (To be able to investigate properly, we will need to be able to efficiently reproduce your steps.)
• Provide us with information required to contact you (at least telephone number or email address).

What we promise:

• We will respond to your report within 5 business days of receipt, with our evaluation of the report and an expected resolution date
• We will keep you regularly informed of our progress toward resolving the vulnerability
• Any report submitted in relation to this Responsible Disclosure approach will be handled with great care with regards to the privacy of the reporter. We will not share your personal information with third parties without your permission, unless we are legally required to do so
• If you have followed the above instructions, we will not take any legal action against you regarding the report

Rewards and attribution:

• MTN does not compensate individuals or organisations for identifying potential or confirmed vulnerabilities.
• If you agree, we'll publicly attribute the finding to your name in our Hall of Fame

• Please do not ask for a reward before sharing the vulnerability, as we need to evaluate your report before responding
• If you report a vulnerability that is unknown to us, and if you are not from a country where we are prohibited by law from making payments (e.g. due to sanctions), we may decide to offer you a reward based upon our assessment of the criticality of the vulnerability
• If you agree, we'll publicly attribute the finding to your name in our Hall of Fame

Acquisitions:

For all our acquisitions, in order to give our development and security teams time for internal review and remediation, we will introduce a six-month blackout period. Bugs reported in that period will not qualify for a reward

Out of scope vulnerabilities:

• Vulnerabilities affecting users of outdated or unsupported browsers or platforms
• Issues that require unlikely user interaction
• Clickjacking/UI Redressing
• Reflected file download
• Verbose error pages (without proof of exploitability)
• SSL/TLS Best Practices
• Incomplete/Missing SPF/DKIM
• Fingerprinting / banner disclosure on common/public services
• Disclosure of known public files or directories, (e.g. robots.txt)
• Content spoofing (text injection)
• Tabnabbing
• OPTIONS HTTP method enabled

Response Efficiency

9 days
Average time to first response

10 days
Average time to triage

2 months
Average time to resolution

● 69% of reports
Meet response standards
Based on last 90 days

Program Statistics

Updated Daily

433
Reports received in the last 90 days

5 days ago
Last report resolved

4258
Reports resolved

812
Hackers thanked

Top hackers

harrisoft
Reputation:7292

sheikhrishad0
Reputation:1374

badcracker
Reputation:1323

emade0x90
Reputation:877

z3ck3bug
Reputation:804

- Recently disclosed 0-day vulnerabilities
- Presence of autocomplete attribute on web forms
- Use of a known-vulnerable library (without proof of exploitability)

Last updated on December 18, 2019. View changes

Looking for what's in scope? Check out the new Scope tab above.

All Hackers