mettle.

Responsible Disclosure

V1.2 – July 2023

Changes to the way we use your information

At Mettle, we're big believers in protecting your privacy and security and we value the work performed by security researchers who work tirelessly to make the internet a safer place.

We operate a policy of responsible disclosure whereby our Security Team work closely with researchers to ensure all vulnerabilities submitted to us are reviewed and fixed as appropriate.

To support this policy, we also run a bug bounty program that rewards researchers for responsibly disclosing any vulnerabilities. More information about this can be found here: https://bugcrowd.com/mettle.

If you believe you have identified a security vulnerability in one of our products, services, applications or systems, then we would love to work with you to fix it as quickly as possible.

When to report a security vulnerability?

If you think you have identified a security vulnerability that affects Mettle systems and/or customers then you should submit a report as soon as possible.

Guidelines

We request that all researchers follow the straight forward guidelines below:

- Do not publicise the vulnerability without our explicit approval
- Do not access customer or employee personal information or any Mettle confidential information. If you accidentally access any of these, please stop testing and submit the vulnerability immediately
- Stop testing and report the issue immediately if you gain access to any non-public application or non-public credentials
- Do not degrade the Mettle platform (e.g. Denial of Service), customer experience, disrupt production systems, or destroy data during your research
- Do not run automated vulnerability scans – we have the capability to do this ourselves
- Securely delete all data retrieved during your research as soon as it is no longer required, or as otherwise required by data protection laws

Legal information

This policy does not give you permission to act in any manner that is inconsistent with the law, or which might cause Mettle or partner organisations to be in breach of any legal obligations.

What information should you provide in the report?

The more information we have, the faster we will be able to respond and fix any vulnerabilities that may exist. The below information is a loose template we ask researchers to follow when reporting vulnerabilities:

- Your name
- Date and time of discovery
- Phone number (a way of immediately contacting you would be incredibly useful in the event of a serious vulnerability)
- Technical details of the vulnerability
- Clear and concise step-by-step guide to allow for validations (screenshots and/or privately attached videos are always welcome. Please do not use a public image/video hosting service such as YouTube)
- Trace dump/HTTP request/response where appropriate

Reports that are out of scope and that are unlikely to facilitate a response

We receive a lot of spam-like disclosures which are out of scope or are low effort. We recommend you avoid sending us a report of any of these, unless you believe it deserves an exception:

- Reports that are not actual security vulnerabilities (like forgetting your password)
- Spamming, social engineering, or phishing attacks
- Physical exploits and/or attacks on our physical infrastructure
- Accessible, non-sensitive files and directories (like README.txt, robots.txt, etc)
- Fingerprinting/banner/version disclosure of common applications and/or services
- Username/email enumeration by bruteforcing or by inference of certain error messages – except in exceptional circumstances such as the ability to enumerate phone numbers by incrementing a variable

More about our criteria can be found here: **https://bugcrowd.com/mettle**

What to expect when you report a vulnerability

You should receive an acknowledgement email once we have picked up your report. We aim to triage this within five working days and let you know what we're going to do next.

We'll then prioritise and remediate the vulnerability. The time this will take depends on the complexity of the solution. Feel free to enquire about the status, but please avoid doing so more than once every 14 days.

We will let you know when the vulnerability is remediated, and you may be invited to confirm that the solution works.

Now that you've read the above, here's how you can contact us

We offer two methods for reporting a vulnerability. You can either:

- Submit your vulnerability to our bug bounty program: **https://bugcrowd.com/mettle**
- Send through your report to **security@mettle.co.uk**

A responsible disclosure to either one of these is eligible for reward if it meets the reward criteria. We reserve the right not to pay a reward for reports that provide insufficient information, in our view are not of value, or don't relate to genuine security vulnerabilities.

If your report contains sensitive data, then we request that you use our public PGP key which can be found below.

PGP key for responsible disclosure

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGOA4ywBEADCA4rGLAzCqyAlYwVe3OaWf8pylAOsp8VLhJmWn+U3jv+rSNpL

G60JIRzua1/NvqOxkhY2Lq+udZaB7iGZndZRY6s7SvjO9Su2gO57K1WsMkZL2i7y

yUD/oT2ivwX2txOvlaJxl6RcXUAJmMOMDWes82Zm99NySb1cWvtI215/cmYUZl0R

PEG29gNA5×3vaD/Zixle+TNsCOISuUXvDiK0wTkvxhiEl/H80YRr26/IfJHJS7CD

xkoJWcvjpw3eZacHRymdHlrZbiketBffxNUbMsKJcloLTDtrsWDwR977wn76Euym

TJybVhbYci1DZQ2QEbpQJu//8n1Ajd5+ECnGo1Z026f4RjOqrzK8BGaIZqyc5lhO

aPbRNjyvVmgeT0HsTLyWYMCqhEhhBjiZrukOwTOnUMA5Wu0LL8TO/7/Dqqq1jAVi

7SpacfiprAgf/j3grg6eyGLdNHivUcond5Urr6w3lJX4A+6ePIEwMaFxlzR0Xtgd

BW3nUs9D7TeFJkFAM7fC9FwzOw2S1jRsTXfA2j2khYk/FXcxQUWgCE8TyT5BAJTX

yhk/QAcCdBhGF0MBHL6vDqH/NEIzNDzvfWxQ6GUo0N9tNuYESGtvaifeShwRdDxt

Sm5rUP8JKF/xh2fas3uBqp2k2dhfa2ump+6HiWUmTPwn7fl5DxLfrLygJQARAQAB

tDtNZXR0bGUgVmVudHVyZXMgTHRkIChCdWcgQm91bnR5KSAoKSA8c2VjdXJpdHlA

bWV0dGxlLmNvLnVrPokCTgQTAQgAOAIbAwULCQgHAgYVCgkICwIEFgIDAQIeAQIX

gBYhBPQ7JPnMWKDX5V8LqexBJxOs554UBQJjgOXGAAoJEOxBJxOs554Uh4QP/2k/

X1OJs+pCLN6x/wG/cI7MEVLXOl+cP5mWirp0s2C6pnBBZilbLD83gLJRNWskRMAD

CFhpp+oeEHj/+ciW7J7sMVvhstsnbn3blmB9ot2+YtnJvMOB8hgOjhzmm5MndoWP

pGZ2lqYZacXwUHVQ27GTsNRzLxH4rqLblTVNZgKKP1hv++DQ/dM53occXRi9I4FG

YPHpdEY+UsxTj+L8qlnFCis2vBxm/epH1UtObtf+RaUKW8YWvOF+EzpvIdQTDWFv
s7e7tg2mi0KzZXCqUOCaSgKkU21qtV3B+QsRg2SCvz9/enB8BfbVPJbcWHDLwPS9
PXWybPWhJQcD7u0luzNiwYwdkXNiDEq2Nfn6bCP57uROL86Py7qpUfNzfKAtgZgx
B+ylNZNtehe+4vuJup6a2kAv/n9bwGXf7upk3nYshb3Vnpj8o3R6DDTp9boiS6gT
pWdPIdNNSWdzk6iCTtEjj4JSmYXlZ8Jy0lhVkD3nUDoN0p9UPnLi0sV0AJIt6pM8
Fc2AnPEgko4vkTO5zP0hC4YYseryoPpACv8qHhVO18oTnCEXM67lRDZrblmlwZ7w
39iG/UmbXeyFV6YIFLDL8kp+150X8dG9ih7srIrQjjIrElB2xJv4xTu0×07tya27
zpfK285TRYg1lA6xaBjdbtzwLG8xZpuMTeLf89ZbuQINBGOA4ywBEADmp9jm4bnU
5ZXOOCScv8KHSRVOE+4J5mbXrgdWYHv4WXOPqPHTNQ+LC8pX/s4BwBdy6v0RwuAm
POHbyEPSHYiUpjkPXbXYdC5guS8Se9vUqMzCsRqDEu9LeEJ++9VNwNos6wfwtRu5
0WrSTg0GWRQCiMhBC3hTowIT5lLmsVszpoUWdMJCzH3VOBAfbPOPPg/OFh6VELbU
pLFtH7HhdpelNdyXfQa7uA+EeHrcB1Us2GNSRzUuAMp10+ZE1g1pQMS3C4YLPbUs
/La+glNmiqtzzNHRmir7z5ACf7l57aJnDQCMo22CRx/aLCDJHuioomQ4v+zwTv7r
b6/4tqHWRMRUl69NyDlWbdoeIj1D2Fji/BpvSPvKtI9X+1UZAksmc/yesx5h/sFn
A4NGU6avFw95OI/3zurlDGrqkTrlypoFyEutobifSQdSirYngaYe1qGrk0XYlS9/
GcXF5MI89GltnoGj3j3En6Uq1vAkK0A7BTE/VR+ANZIB3bfWdmzAmI62vEqQsUUK
ST1vyTgHL5QTQ8dO21hEESTiVDC5ZOJqiqAykfEK+B/O3xt+2l4dSMSSolNPPC3z
xZd3ag1GH7pMnIboFGAj3DoPJwF1iyx6aqdwOqLjCj3SgpD7aLp0e6ew1C5wjr+Z
o46pdNA+InsyMwC8DkemTgg+PUZAUnq9swARAQABiQI8BBgBCAAmFiEE9Dsk+cxY
oNflXwup7EEnE6znnhQFAmOA4ywCGwwFCQeGHzYACgkQ7EEnE6znnhS68Q/9GjbW
2tgTdcCLAY2bUpRRxwWFd2NzArhpdzK4NjENfdrzGG6KgnwaJLq5FVThFgs7UAva
9ioFDLX0r8utnMaY1jcA5BqKc05jvpIV4b6V1MeXB49JK2DF47aGKv21Be/03XrU
4bXZ2xsKbc0kqG1cdhZKKSQa22bvtOrpUtl3EoS9Ughery/xPSwU9zPebU7iIl11
l2sXVy21xzCXoGJe5BSW50/kv6Y+ZdiNKUvHNaqbFQG+dSmKPmol78k7kdVCQjAQ
srelKzWT+8gm+rfUqhzynzHfQOTWxyi7NrRWpdIDVT1QyXfepElH8kR65/EfUuIW
XicraxB7cz1rayleQeVpiZJAD8Qk589JzxAryLCWlIBi8b1F2w48j1DjcPAlhD2U
VAzhR6oDvZmOmieS32lCXAdNKvazlmR9DG1XOZNSkP+GfEkwrycbkgJXnpzFlVtu
vVTW0nJIGjIPxeBeDS/T3xivsZOHrBVe030tr/2lDCA+KXYuhu3PScbemIiEhOtm
dPpnnm8TVz3Il7imC5+TH6F2qf3PCaadUJo68b33ZVZNIC/DvL4/OCZw0HxpGGn7
2DMgsyEucoTVNYuVrsAd40G15uYXQK+D5thRUKZxQo8QbuOJTH6p4FkxLyL4cx3l
kykEWhw55b8SSjkiAFZ73/5edO/y15L51EHBxy8=
=lH6W
-----END PGP PUBLIC KEY BLOCK-----