Responsible Disclosure

V1.3 – March 2025

Responsible Disclosure

V1.3 - March 2025

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 which means our Security Team works closely with researchers to make sure all vulnerabilities submitted to us are reviewed and fixed as appropriate.

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the "Organisation"). We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: security@mettle.co.uk.
In your report please include details of:
* The website, IP, application, or page where the vulnerability can be observed.
* A brief description of the type of vulnerability, for example; "XSS vulnerability".
* Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress. Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to inquire about the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate public release with us.

Guidance

You must NOT:
* Break any applicable law or regulations.
* Access unnecessary, excessive or significant amounts of data.
* Modify data in the Organisation's systems or services.
* Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
* Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
* Disrupt the Organisation's services or systems.
* Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers.
* Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
* Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
* Social engineer, ‘phish’ or physically attack the Organisation's staff or infrastructure.
* Demand financial compensation in order to disclose any vulnerabilities.

You must:
* Always comply with data protection rules and must not violate the privacy of the Organisation’s users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
* Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organisation or partner organisations to be in breach of any legal obligations.

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
G60JlRzua1/NvqOxkhY2Lq+udZaB7iGZndZRY6s7SvjO9Su2gO57K1WsMkZL2i7y
yUD/oT2ivwX2txOvlaJxl6RcXUAJmMOMDWes82Zm99NySb1cWvtI215/cmYUZl0R
PEG29gNA5x3vaD/Zixle+TNsCOISuUXvDiK0wTkvxhiEl/H80YRr26/IfJHJS7CD
xkoJWcvjpw3eZacHRymdHlrZbiketBffxNUbMsKJcloLTDtrsWDwR977wn76Euym
TJybVhbYci1DZQ2QEbpQJu//8n1Ajd5+ECnGo1Z026f4RjOqrzK8BGaIZqyc5lhO

aPbRNjyvVmgeT0HsTLyWYMCqhEhhBjiZrukOwTOnUMA5Wu0LL8TO/7/Dqqq1jAVi
7SpacfiprAgf/j3grg6eyGLdNHivUcond5Urr6w3lJX4A+6ePIEwMaFxIzR0Xtgd
BW3nUs9D7TeFJkFAM7fC9FwzOw2S1jRsTXfA2j2khYk/FXcxQUWgCE8TyT5BAJTX
yhk/QAcCdBhGF0MBHL6vDqH/NEIzNDzvfWxQ6GUo0N9tNuYESGtvaifeShwRdDxt
Sm5rUP8JKF/xh2fas3uBqp2k2dhfa2ump+6HiWUmTPwn7fl5DxLfrLygJQARAQAB
tDtNZXR0bGUgVmVudHVyZXMgTHRkIChCdWcgQm91bnR5KSAoKSA8c2VjdXJpdHlA
bWV0dGxlLmNvLnVrPokCTgQTAQgAOAIbAwULCQgHAgYVCgkICwIEFgIDAQIeAQIX
gBYhBPQ7JPnMWKDX5V8LqexBJxOs554UBQJjgOXGAAoJEOxBJxOs554Uh4QP/2k/
X1OJs+pCLN6x/wG/cI7MEVLXOI+cP5mWirp0s2C6pnBBZilbLD83gLJRNWskRMAD
CFhpp+oeEHj/+ciW7J7sMVvhstsnbn3blmB9ot2+YtnJvMOB8hgOjhzmm5MndoWP
pGZ2lqYZacXwUHVQ27GTsNRzLxH4rqLbITVNZgKKP1hv++DQ/dM53occXRi9I4FG
YPHpdEY+UsxTj+L8qlnFCis2vBxm/epH1UtObtf+RaUKW8YWvOF+EzpvIdQTDWFv
s7e7tg2mi0KzZXCqUOCaSgKkU21qtV3B+QsRg2SCvz9/enB8BfbVPJbcWHDLwPS9
PXWybPWhJQcD7u0luzNiwYwdkXNiDEq2Nfn6bCP57uROL86Py7qpUfNzfKAtgZgx
B+ylNZNtehe+4vuJup6a2kAv/n9bwGXf7upk3nYshb3Vnpj8o3R6DDTp9boiS6gT
pWdPIdNNSWdzk6iCTtEjj4JSmYXlZ8Jy0lhVkD3nUDoN0p9UPnLi0sV0AJIt6pM8
Fc2AnPEgko4vkTO5zP0hC4YYseryoPpACv8qHhVO18oTnCEXM67lRDZrblmIwZ7w
39iG/UmbXeyFV6YIFLDL8kp+150X8dG9ih7srIrQjjIrElB2xJv4xTu0x07tya27
zpfK285TRYg1IA6xaBjdbtzwLG8xZpuMTeLf89ZbuQINBGOA4ywBEADmp9jm4bnU
5ZXOOCScv8KHSRVOE+4J5mbXrgdWYHv4WXOPqPHTNQ+LC8pX/s4BwBdy6v0RwuAm
POHbyEPSHYiUpjkPXbXYdC5guS8Se9vUqMzCsRqDEu9LeEJ++9VNwNos6wfwtRu5
0WrSTg0GWRQCiMhBC3hTowIT5lLmsVszpoUWdMJCzH3VOBAfbPOPPg/OFh6VELbU
pLFtH7HhdpelNdyXfQa7uA+EeHrcB1Us2GNSRzUuAMp10+ZE1g1pQMS3C4YLPbUs
/La+gINmiqtzzNHRmir7z5ACf7l57aJnDQCMo22CRx/aLCDJHuioomQ4v+zwTv7r
b6/4tqHWRMRUl69NyDlWbdoeIj1D2Fji/BpvSPvKtI9X+1UZAksmc/yesx5h/sFn
A4NGU6avFw95OI/3zurlDGrqkTrlypoFyEutobifSQdSirYngaYe1qGrk0XYlS9/
GcXF5MI89GltnoGj3j3En6Uq1vAkK0A7BTE/VR+ANZIB3bfWdmzAmI62vEqQsUUK
ST1vyTgHL5QTQ8dO21hEESTiVDC5ZOJqiqAykfEK+B/O3xt+2l4dSMSSolNPPC3z
xZd3ag1GH7pMnIboFGAj3DoPJwF1iyx6aqdwOqLjCj3SgpD7aLp0e6ew1C5wjr+Z
o46pdNA+lnsyMwC8DkemTgg+PUZAUnq9swARAQABiQI8BBgBCAAmFiEE9Dsk+cxY
oNflXwup7EEnE6znnhQFAmOA4ywCGwwFCQeGHzYACgkQ7EEnE6znnhS68Q/9GjbW
2tgTdcCLAY2bUpRRxwWFd2NzArhpdzK4NjENfdrzGG6KgnwaJLq5FVThFgs7UAva
9ioFDLX0r8utnMaY1jcA5BqKc05jvpIV4b6V1MeXB49JK2DF47aGKv21Be/03XrU
4bXZ2xsKbc0kqG1cdhZKKSQa22bvtOrpUtl3EoS9Ughery/xPSwU9zPebU7iII11
I2sXVy21xzCXoGJe5BSW50/kv6Y+ZdiNKUvHNaqbFQG+dSmKPmol78k7kdVCQjAQ
srelKzWT+8gm+rfUqhzynzHfQOTWxyi7NrRWpdIDVT1QyXfepEIH8kR65/EfUuIW
XicraxB7cz1rayleQeVpiZJAD8Qk589JzxAryLCWlIBi8b1F2w48j1DjcPAlhD2U
VAzhR6oDvZmOmieS32ICXAdNKvazlmR9DG1XOZNSkP+GfEkwrycbkgJXnpzFlVtu
vVTW0nJIGjIPxeBeDS/T3xivsZOHrBVe030tr/2lDCA+KXYuhu3PScbemIiEhOtm
dPpnnm8TVz3Il7imC5+TH6F2qf3PCaadUJo68b33ZVZNIC/DvL4/OCZw0HxpGGn7
2DMgsyEucoTVNYuVrsAd40G15uYXQK+D5thRUKZxQo8QbuOJTH6p4FkxLyL4cx3l
kykEWhw55b8SSjkiAFZ73/5edO/y15L51EHBxy8=
=lH6W
-----END PGP PUBLIC KEY BLOCK-----