Responsible Disclosure

V1.1 – August 2019

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.

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.

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:

- Name
- Date and time of discovery
- Number (a way of immediately contacting you would be useful in the event of a serious vulnerability)
- Technical details of the vulnerability
- Clear and concise step-by-step guide to allow for validation (screenshots and/or privately attached videos are always welcome - please do NOT use a public image/video hosting service such as YouTube as this will upset our legal team. We don't want to upset our legal team!
- Trace dump/HTTP request/response where appropriate

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

- Reports that are not actual security vulnerabilities (e.g., forgetting your password is not a security vulnerability)
- Spamming, social engineering, or phishing attacks
- Physical exploits and/or attacks on our physical infrastructure
- Accessible, non-sensitive files and directories (e.g., 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

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

Send through your report to security@mettle.co.uk

If your report contains highly sensitive data then we request that you use our PGP key which can be found here:

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

mDMEXJOj5xYJKwYBBAHaRw8BAQdAOkv5olKSU1KXhp/J6VCfQizOMz53hHKm4uq4
y1nQo9u0M01ldHRsZSBJbmZvcm1hdGlvbiBTZWN1cml0eSA8c2VjdXJpdHlAbWV0
dGxlLmNvLnVrPoiQBBMWCAA4FiEEhSu2WIdwGO9efkFWDuHlCRKBUUAFAlyTo+cC
GwMFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQDuHlCRKBUUB8rgEAjrIemEwt
t1nzEfXUObbIdTZ3lXh6jlMRukcKKgkck/cA/0Vi33AD+2Yqul38dBwFvqaazL+s
rPT10rH7iTPFgU8MuDgEXJOj5xIKKwYBBAGXVQEFAQEHQNQn+RuiOVX2CEENXeFz
3qbcOi5iGDXTuvgttmm1S9ttAwEIB4h4BBgWCAAgFiEEhSu2WIdwGO9efkFWDuHl
CRKBUUAFAlyTo+cCGwwACgkQDuHlCRKBUUAFgAD/YheO8CYHqBxh07X3kAnO5Ipv
PEGXb5EnCAL534FMEP8BAJNTOHdfpOr3kcS47v/07UzaQle2alUJ3MfeAR0q+MoO
=nV31
-----END PGP PUBLIC KEY BLOCK-----