COTX Vulnerability Disclosure Policy

Introduction

COTX Company takes the security of our systems seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

We encourage you to contact us to report potential vulnerabilities in our systems.

Guidelines

We require that all researchers:

- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command-line access, or use the exploit to pivot to other systems.
- Notify us as soon as possible after discovering an actual or potential security issue. Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.
- Provide us a reasonable amount of time to resolve the issue before disclosing it publicly.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- Use the identified communication channels to report vulnerability information to us; and
- Keep information about any vulnerabilities you've discovered confidential between yourself and us until we've resolved the issue.

If you follow these guidelines when reporting an issue to us, we commit to work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission).

In the interest of the safety of our users, staff, the Internet at large, and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g., open doors, tailgating);
- Findings derived primarily from social engineering (e.g., phishing, vishing);
- UI and UX bugs and spelling mistakes; and
- Network-level Denial of Service (DoS/DDoS) vulnerabilities

Things we do not want to receive:

- Personally identifiable information (PII)
- Personal Payment Information

Reporting a vulnerability

If you believe you've found a security vulnerability in one of our products or platforms, please send it to us by emailing **security@cotxnetworks.com**. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability; and
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us).

If you'd like to encrypt the information, please use our PGP key.

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

xsFNBGITcWoBEAC1K2K9VCzDdr6JbK+ndgWwvBNpiDLs/bWZO2BVyTz0/lHH
02HFXRXPaKcsHOJWBd1lfVwIlW3wdSDvAjl1ZltasQ3Ua6wqc6npRdMTHL61
lbZVJWgpNdFtkK29yDlofkuVn59JD6WTYah+YhpgDhnUyIMfWEj50k7fbtXp
yRL7QyNvhGXnGlvG9B3OQzJExd4iJl4Ydf33zDOoAuy2NKK55nHwuz1olx+H
5XnbTutG+Nd0Jza5e6Qfhd+J21sr0DuE7VVGoxcwQjvo+dQm6lM8GoO4F5uW
yDOn1oilWcTCm4sYtvdO/KvT4Ugqwq/HOZu5tV2fWTvkra+khZ/ffTvL/maa
+EjuohZlD6c6Z4WMzFeHr4/LGGlGUd99yD52ZNpgGtvmylrxiPvtl6heUCrF
xaBw56LHVq2lYqyhKAWoTUyXuvHb5rTYhfURjFYW6HzTJSOiflCvDYETnaTt
1DFcinhFn7dW7U8/YfLxHvSxoZjhRTUdzTzDc/Hn6+6nn45Nlf8PE0nwZASW
RRpGys1TwDODrFdWVDZjYbhMlZRCCrlvjYR0jTurmlRlqaRG6gac9RUknL4g
W3iJRcj+ovyQQTkDJqUcdPNJMugiVMFh8UKlpLMJWhQ3RqVjmA+0vBw4GCXc
VC9v/EWNBYNTmxW8UA3cwqqxGT4ZG1sfO/aatQARAQABzQDCwYoEEAEIAB0F
AmITcWoECwkHCAMVCAoEFgIBAAIZAQIbAwIeAQAhCRCGX2IYI3wEthYhBKYE
aDgCd/PXLdabXlZfYhgjfAS2KYQQAITaqRAYErpUTRglmfGn7yvZ3WpJBFKd
KY+cXvgVLEht5L5SBuLUPym/W2Mpj+dPezOz3ctp8r7KkuY7m0idlOKUMRht
SUnjyLueCO7PrNkKCjsnO4kVNPBP12SxATE4jfiVXrC/GCX9v8FPGFpZvJVr
RLNDK44ODAgQ5R+wYfMz5F2XsxEtuhnaQbhMgqlpdgdBoQ3cmjbpINfCxT/C
Z7BEwGtN2HVX9AA3OQX2JWFPrzZtCcqu8F/sTWmtPxLOd8V3wvLZyRVLMwn+
iyDpjqZigcaPWka+wcsslEg/Apcq2wEoXPrzoxka6vHbaJgkl7uw1EtE/TSO
DA5/504cbOAEjSplFaLI2RNWSOs9ZFBrdXlzp0iwjzgnbnBtuWeym+Q8DfxZ
VYjpY/uDuPlborsiXcJvo3jbZz9RnHJNM8tqKzYbETx0wGzbwWvs0k0ib8lg
U9YSmFomHoc9T+thSHQtX6kesdifAdbtffWe//UVx4+oL4tzSJVGEfFaJ1vs
Aljp8M/+wnC2XCXMxIrAPlMcPo2yMdBK3h1PvowXPDGa9aD3tJnceG556gDZ
5LQBj0R76ZvCGmbACWbNe1m7Gxlj7qseXAPhWmMba33IdxxXSb3COY5d5xEK
HO5pPPNvJj2uDlg6+qwOa7g7eqcbxVfTCbRT0qANXBROYVjQRjT5zsFNBGIT
cWoBEADGsoNsCQStz66PC/XwzdoGvxwXYYYDATfVYgkT44ztFnJajUrD7fZp
9vGoN2b0mhY+zhcS2xSg5Ypp5GZjn6mMNelCYL3Tfk2dfQxI5VNBLVLLShPS
YX3hrsIntNZA3F5pq4kmN3/6/5XOQd1X1Qz8SnidffK5T1+8NpqKbwyLsHYY
fSHFznnI7jDdlcDTSlq9B/4NsT0JXxlVclSogbS9LEmcen+osmK5rDE0BhRe
brSdlxo+DXX6hnWXwnm27LzPJAjeb9M1erBEdLf3fEmyH4MEV8p/zAA++K57
bezgEqd7wEczjcLiDnK272hNPuT+05cUWUa1Zt89lXH8YWia2k+0R479vx8u
UWDet81i9lSKnWx0Ggu5On65pz6W41M680FakkBz3Le/Hw0omsh22/ekz/KU
7sTURLGlfBce8YErJXOx4gBpG2L64Z3EnfE8qEGw05tbjq30Z5XKg/Lo8FDX
qfB55xh+tL7A7OcfE9aU8Mmv+62Awa/SdHF/PsdbDNlgk/y529oLJ+c+8FxW
dHrZ4bUDkEWDjrLKccPZ3trh4h5uTh8w36sResswKdea8jw9RnqdAPwbJxHu
Ut/l11xGhf9uaWOCdKUvSPvOFPAJkdCqg6b/VJBYPWVe3dGtkmbDNn01Xz6N
Gie5Tuy51nfmvNLWmq7M1ShKkjaFqQARAQABwsF2BBgBCAAJBQJiE3FqAhsM
ACEJEIZfYhgjfAS2FiEEpgRoOAJ389ct1ptchI9iGCN8BLaSww/7BPZuvEDw

qSofujvdWJ/Sn3bjTFc/HDc2×5Ta+LJZq65jdP6TZ/JwTmGYqsayUDa0778y
235Dh5nuWatzbBEouZMxLnDh1FSypedigShxO6M4Sow7Ql0swDFLi5frOOCl
XPTVZdI3xsYC+cHo4qaaLDXjsgx3XWHa3NFW+QbtokR1Tg9vv3c/7SM/CGkj
lQmj3PCxCicquszmqRk8HMlaylUAyiVSEHCHULxHhuBUVWri2a4qlDE5FlQ8
XNX9eGAy5oiie7KXyC0KsELPnhGgj6CxjQ3MLM7GiEf/vE5bGeXDPf4yGoa3
MZoNG0jev8AQnfz1HDmkQhWi80AzYkQba1sud5BkXJQ3l+M79lQf3h5by7S4
mo6iuS7/qtiyX7bWcplEannEsVi2ncKZyXGgmXB4/blgbZZUgfyZd8RSjz6R
fMSBPUOnm4f8uedKFekLx2Sm0SDGvpoAXlHsL9Ea4xKRXh8j/cZYX2L7QqyP
X04DhEma/HtWoHkiZGvaCpX+ZJsgDbcuaCqqOTPwqoxZf1B+M+xWh73mavNX
BhqBu1RfNvf8QOLKFalfH+BvtI3ekNnfXz4G73V5W2BOfu04+f93TTSPrFX1
JmgcSCARMZeJtmudVEuRZEZb47+gJ2Xr8Ahe4M6vaaTqRJ/z65n1uCt67MdI
7zC4n51UrkcnYJQ=
=rFuj
-----END PGP PUBLIC KEY BLOCK-----

What we would like to see from you

To help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and quickly as possible.

- Within three business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Questions

May send questions regarding this policy to **security@cotxnetworks.com**. We also invite you to contact us with suggestions for improving this policy.