Bentley Systems' Responsible Disclosure Program Guidelines

2020-06-26

Department: Application Security Team
Information class: Public

At Bentley Systems we take the security of our systems and products seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users.

1 Generic Guidelines

Bentley Systems requires that all researchers:

- Avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- Perform research only within the scope set out below;
- Use the communication channels defined below to report vulnerability information to us;
- Keep information about any vulnerabilities you have discovered confidential between yourself and Bentley Systems until it is fixed.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly.

2 Code of Conduct and Legal Responsibilities

When conducting vulnerability research according to this policy, we consider this research to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms & Conditions that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy;
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our communication channels defined below before going any further.

3 Scope

- All *.bentley.com subdomains (except **communities.bentley.com, bentley.matrixlms.com**) *
- All Bentley Systems desktop products (Only CONNECT Edition and Later)
- All Bentley Systems mobile apps
- All Bentley Cloud Applications and Services
- All Bentley Open Source Projects (including imodeljs.org)

* *Communities reports should be submitted directly to Telligent.*

* *Synchro Academy reports should be submitted directly to Cypher Learning***.**

4 Out of Scope

- Bentley Systems' Infrastructure (e.g. VPN, Mail Server, SharePoint, Skype, etc.)
- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- Findings from applications or systems not listed in the 'Scope' section
- UI and UX bugs and spelling mistakes
- Network level Denial of Service (DoS/DDoS) vulnerabilities
- Any services hosted by 3rd party providers and services are excluded from scope

IMPORTANT NOTE. It is forbidden to send emails to other address than security@bentley.com.

5 How to report

If you believe you've found a security vulnerability in one of our products or platforms please send it to us by filling the Trust Center's Form https://www.bentley.com/en/about-us/contact-us/contact-us-form?topic=11 or send an email to security@bentley.com.

We prefer that you use our public **PGP key** (see Appendix 1) to protect the information you send over.

Make sure to have included the following information:

- Detailed description of the vulnerability containing such info as URL, full HTTP request/response and type of vulnerability.

- The necessary information that we need in order to reproduce the issue.
- If applicable, a screenshot of the vulnerability you have found and/or a video.
- Contact information, name, email, phone number, and your public PGP key (if you have one).

6 Rules of Engagement

- DoS is strictly forbidden.
- Any form of credentials brute forcing is strictly forbidden.
- The public disclosure of a reported vulnerability before it has been fixed (within the grace period) is forbidden.
- Do not destroy or degrade our performances or violate the privacy or integrity of users or their data.
- Exploiting vulnerabilities, besides a generic PoC, is strictly forbidden and will be prosecuted according to the applicable laws.
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information.
- Do not engage in extortion (i.e. Claims for compensation as a condition for sending in a vulnerability will not be tolerated.).

7 Public disclosure

Unless otherwise informed of the resolution of the vulnerability, we ask the researcher to withhold for a period of 90 days before publicly disclosing the vulnerability. Failure to do so could result in legal actions.

8 Eligible Vulnerabilities

- SQL Injection
- Remote Code Execution
- Cross-Site Request Forgery
- Directory Traversal
- Cross-Site Scripting
- Sensitive data exposure
- Authentication Bypass
- Privilege Escalation
- Business Logic Issues
- Subdomain takeover*

** Please report only after you see that subdomain is free at least for 1h. Actual takeover of reported subdomain as PoC is forbidden.*

9 Exclusions

- Security issues related to **https://communities.bentley.com, https://bentley.matrixlms.com/**. *****
- Publicly-released bugs in internet software within 15 days of their disclosure.
- Spam or Social Engineering techniques, including SPF and DKIM issues.
- CSRF without any security impact (e.g. Logout CSRF).
- Self-XSS (we require evidence on how the XSS can be used to attack another user).
- X-Frame-Options related (clickjacking).
- Missing cookie flags on non-sensitive cookies.
- Missing security headers which do not lead directly to a vulnerability (unless you deliver a PoC).
- Header injection, unless you can show how they can lead to stealing user data.
- Version exposure (unless you deliver a PoC of working exploit).
- Issues that are non-exploitable but lead to crashes, stack trace and similar information leak, or stability issues.
- Denial of Service.
- Anything requiring outdated browsers, platforms, or crypto (i.e. TLS BEAST, POODLE, etc).

- Anything from an automated scan, anything that is already public, or anything not under Bentley Systems control (e.g. Google Analytics, etc.).
- Theoretical issues that lack practical severity.

** Communities: If you would like to report, you should do it directly to Telligent.*
** SYNCHRO Academy: If you would like to report, you should do it directly to Cypher Learning.*

10 Duplicates

In case of multiple researchers reporting a similar issue in different time frames, only the first one reported will be considered.

11 Vulnerabilities Triage

Once the email will be received:

- The vulnerability will be analyzed;
- We'll look at your submission and, if it's valid, hasn't yet been reported and meets requirements of our bug bounty program, you may get a compensation for your efforts;
- You will be informed when the issue is fixed.

12 Rewards

Vulnerability Examples	Price Range (USD)**
Remote command execution	$500
SQL injection (without RCE)	$200-400
Privilege Escalation	$200-400
Improper Authentication	$200-400
Improper Access Control	$200-400
Insecure Direct Object Reference	$200-400
Cross-Site Request Forgery	$100-200
Server-Side Request Forgery	$100-200
XSS	$50-150
Subdomain Takeover	$100
Sensitive Data Exposure	$50-500
Unimportant Information Disclosure (e.g. stack trace, IIS version, useless path)	$0
Clickjacking	$0
Content injection in error pages	$0
Unexploitable crash or any report without proof of exploitability	$0
Others	$0-$500

***Note that multiple instances of the same issue will only be rewarded to a max of 3x the price.*

We reserve the right to change this table at any time and for any reason. We do not guarantee you'll get a reward even for valid report. We cannot give reward in US embargoed countries. We only pay through PayPal.

Bentley Systems reserves the right to withdraw the bug bounty program and its rewards system, at any time.

12 Appendix 1

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

mQENBFurbqsBCADK2sHGqlxjkxbU9c3wzzvWIT4l2qYgL/cmB9VK9xOOhqj/gU8y
pPWS6InRa/00Z8FC4TM6apXRM4kmu6b4sUTrTEtH68GOuIBxxZwFrB1pV20VVdvX
adBNd4Niu4Z4lHBWjnf8lfgLkw8CwD/DrDtJbEetgm424UzWaILc1J/J1vEEupy1
Ker+uXbAZIk7hla+Hla3PkrWb7m1ZkpZwDL7Rp0sRYK4vlLNaM9ksawoA3oTsMHp
bf0ZREkgbhN23Yqyxi+3o32uR7I0f938mmjCRTp9g11evENi+23J1xNXyczPR0+B
So/bGIRv25x5Kt5nAqb770nB6wJngL7jMz+BABEBAAG0R0JlbnRsZXkgVHJ1c3Qg
Q2VudGVyIChSZXBvcnQgYSBzZWN1cml0eSBjb25jZXJuKSA8c2VjdXJpdHlAYmVu
dGxleS5jb20+iQFOBBMBCAA4FiEEo0CSddTjFAwk2fut7dlDdRt+0GUFAlurbqsC
GwMFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQ7dlDdRt+0GV64Qf8D5d1UKJT
lAu6xMyVX/fPlsN3koYabtj0JdcYVFMKBwDk8Qok4oTd94K2jLJDWUcCsBEHymMp
I7Vc621KlLszHqnQszUyyrUVsYHaXaseGB/OA5d6pEEdbYMqstfMTbjpRe7e2Gzc
6tys4DqQeRfSv2ODEopPOeWk5lGMfNvd6Kwc0P767Gay9ON3kj43WU+7whSyh83H
SRfrxZMqUur2gA7bGCp1F4AQxecGjtGxQ37MnZc4zJVdipYjgkPqdZl1yupsxcid
zyPywNZpoi946is+KIvmBP/JaLvBpO9pJT5nlotjcIu8junFyjxKPuRLTPJPKxV3
vpNXvABd+XLLGLkBDQRbq26rAQgA6NSoYK31fBLXVGRsCnPVc2hF+TEiecBC50py
Ok3xfabAb1G9S47argJVMBUJec/7ANIVRNdh5PadZRWxpBKRptRNp7MDT+GY1lJN
jRWBUEKde4mt4pt7vJaJ2WG9QVrc79VuAqyOXEWqFg/4xO9gNV3g8VfeUz6Ou8xP
8HdimXp97p7Hv7Cqocf/GINi5pNAY70qLFoyBFO2Nk+uMhe8G4uC6S7BtL5FiG74
NWiQK8IbIAxZ47nzm3HVMh1J2RK3D2LelfWrjL5dFbMmnajlM/ZneO8GjHk7dnoP
q3L9J4rfnKF5dvjEensjJdEP8Lfo/GlYF3Colf2wqROq4lAOuQARAQABiQE2BBgB
CAAgFiEEo0CSddTjFAwk2fut7dlDdRt+0GUFAlurbqsCGwwACgkQ7dlDdRt+0GVx
zwgAxaSlkfynG4dppg/58dtgpbw0HSvHwZk/Hgghj+1Bj/qisYthNmco+AuLZI/6
SqlvgAcck/dyYkaMu1EEiGCceGRWk+lNliEOTmcuFw/ZFbARNGCYNJ74MJdNlMCA
Jn81UyS0JoV4K05EWee7M+FP8BGofva68uvbbJl3XeWIioJ5qz7dod9Ij+X3vX7A
ExUTR5/AqUaVEzhiwszRaYO6qC7C4atLyllGh8X1YbZdvL8NZoL9/TkLqD0T6x3f
/zauIONFEfJSRBCOdqlGvzlVUAPW5xmlDCE7SusWTKNtHQF09Lk99R6CUsXuQ3No
WJ5+/TpZ8bdHhaj0CIy75Crcvw==
=4lGy
-----END PGP PUBLIC KEY BLOCK-----