Bentley Systems' Responsible Disclosure Program Guidelines

2023

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 you and Bentley Systems until it is fixed.

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

- Not to pursue or support any legal action related to your research.
- To 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) (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
- 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)

4 Out of Scope

- Bentley Systems' Infrastructure (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
- **https://bentley.matrixlms.com/**
- **https://www.plaxis.ru**
- **https://communities.bentley.com** Communities reports should be submitted directly to Telligent.
- Synchro Academy reports should be submitted directly to Cypher Learning.
- **https://ebook.bentley.com/** Ebook reports should be submitted directly to Impelsys.
- https://yii.bentley.com/en
- https://vshow.on24.com/vshow/bsn012108_ve_01/registration/19990
- https://vshow.on24.com/vshow/bsn012108_ve_01/lobby/19990

5 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*

6 Exclusions

- 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)
- Rate limit vulnerability (unless a valid exploit PoC provided)
- XMLRPC.php file is enabled leading to DoS attack
- 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

*Please report only after you have a PoC in the form of two screenshots with timestamps and a subdomain. These screenshots must prove that subdomain was free for at least for one hour. Scanning tools often catch the short period of time while changes to the subdomain are being executed, which may appear to be a vulnerability but is not: the DNS record is deleted shortly afterward. Submitting the screenshots will avoid reports of false vulnerabilities, saving time for both you and our team.
Reports with a partial PoC (one timestamp proof or none at all) will not be treated as a First report.

NB! Actual takeover of reported subdomain as PoC is forbidden.

7 How to report

If you believe you've found a security vulnerability in one of our products or platforms please send it to security@bentley.com.

Please use our public **PGP key** (see Appendix 1) to protect the information you send.

Make sure to have included the following information:

- Detailed description of the vulnerability containing info such as URL, full HTTP request/response, and type of vulnerability.
- Information necessary to reproduce the issue.
- If applicable, a screenshot and/or video of the vulnerability.
- Contact information, name, email, phone number, location, and your public PGP key (if you have one). **Submissions without this information will not be considered**.
- **IMPORTANT NOTE**. You may only make initial submissions to security@bentley.com. For correspondence after your initial submission, please only reply to the responding team member. If you discover additional information after your initial submission, please wait until our team contacts you and provide the additional information as a reply to that message.

  Enquiries about the progress of the report should be also sent to a team member who contacted you and not to our general email [security@bentley.com].

8 Rules of Engagement

- DoS is strictly prohibited.
- Any form of credentials brute forcing is strictly prohibited.
- Public disclosure of a reported vulnerability with the 15-day grace period before it has been fixed is prohibited.
- You may not destroy or degrade our performance or violate the privacy or integrity of our users and their data.
- Exploiting vulnerabilities (other than a generic PoC) is strictly prohibited and will be prosecuted according to applicable law.
- If a vulnerability provides unintended access to data, you must
    - 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.

- Bentley will not respond to extortion or other coersive, criminal acts (e.g. demands for payment up front in exchange for not exploiting a found vulnerability.

9 Public disclosure

Unless otherwise informed by our team that the vulnerability has been resolved, please withhold public disclosure of the vulnerability for 90 days. Failure to do so will result in legal action.

10 Duplicates

Only the first researcher to report an issue or similar issues will be considered under this policy. This includes reports of the same issue in different environments (e.g., dev-, qa-, prod-)

11 Vulnerabilities Triage

Once your submission is received:

- The reported vulnerability will be analyzed.
- If we determine the submission is valid and meets the requirements of this policy, you may receive compensation.
- You will be informed when the issue is fixed.

12 Compensation

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
Rate limiting on login page	$50
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
Bypass of already reported issue	$25-$50

***Note that multiple instances of the same issue will only be compensated to a max of 3x the price.*
***Reports for an issue in different environments of the product (dev-, qa-, prod-) will be counted as one.*

We reserve the right to change this policy at any time and for any reason, and cannot guarantee compensation for all reports[1]. Compensation is only provided through PayPal.

IMPORTANT. Please make sure to send only a **valid PayPal address**: we will be unable to consider addresses other than the original for payment. If the transaction fails for any reason (i.e. PayPal refuses the transaction; receiving bank cannot accept payment; max amount limit is reached, acceptance of payments only through the website or other instructions, etc.), the payment will be cancelled and **will not be resubmitted.**

Bentley Systems reserves the right to withdraw the Responsible Disclosure Program and its compensation system at any time without prior notice.

[1] Compensation will be provided only in compliance with all applicable law, including sanctions imposed by the United States, European Union, or other jurisdictions. Compensation will not be provided to individuals in countries and regions subject to embargo by the United States, which may change from time to time. Additional identifying information may be requested for compliance with applicable law. Bentley reserves the right to refuse compensation for any reason. [LET ME KNOW IF THIS CATCHALL IS TOO DETERRING]

Project name: Bentley Security
Document name: Responsible Disclosure Program
Version: 1.11

Author: Anushri Aware, Lina Gailiuniene
Department: Application Security Team
Information class: Public

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-----