

**Finding Name: HTTP Headers Expose Detailed Version Information of System Components**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Mohnish Sharma | PT | Senior Team Member | Ontrack |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

Web server default configurations frequently reveal too much about the platform and version of the server in HTTP headers and on error pages. While not inherently hazardous, this information can assist an attacker in concentrating on vulnerabilities related to a particular web server platform or version.

**Risk Rating**  
Impact: Major  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

The identification of the server platform and version, specifically Puma 6.1.1, can significantly impact the application as a whole. Because attackers can use this information disclosure vulnerability to target known vulnerabilities related to the particular web server platform and version, the organization is exposed to potential cyber threats. Such exploitation may have negative effects that include financial losses, harm to one's reputation, and legal responsibilities in addition to unlawful access to confidential data and service interruptions. Furthermore, a breach in the application's security may undermine client trust and confidence, which could lead to a loss of commercial chances.

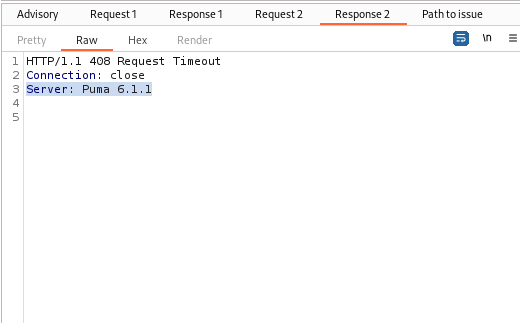
**Affected Assets**

The assets affected by this vulnerability include the deployment environment accessible via the URL http://localhost:3000. This encompasses the entire web application hosted on the specified deployment, including its data, functionalities, and associated infrastructure. The disclosure of server information on this deployment poses a direct risk to the security and integrity of the application and the organization's digital assets

**Evidence**

HTTP response header sent from web server is revealing much information like what type of server it is, its version number. Displaying version information of software information could allow an attacker to determine which vulnerabilities are present in the software, because it can potentially give bad actor hints about exploiting our server, if vulnerability is found in certain puma version.

|  |  |
| --- | --- |
| **Deployment** | http://localhost:3000 |
| **Information Retrieved** | Server: Puma 6.1.1 |

****

**Remediation Advice**

Configure your web server to avoid having it announce its own details.

Remove this header or set non-informative values.

**References**

[**https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/**](https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/)

[**https://cheatsheetseries.owasp.org/cheatsheets/HTTP\_Headers\_Cheat\_Sheet.html#server**](https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#server)

[**https://github.com/puma/puma/blob/7b6301009321d527891e4761da0d39a025b9015f/lib/puma/const.rb#L128**](https://github.com/puma/puma/blob/7b6301009321d527891e4761da0d39a025b9015f/lib/puma/const.rb#L128)

**Contact Details**

Name: Mohnish Sharma

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.