[For Customers Without Backups]

SUBJECT: Security Incident Impacting Your GoDaddy VPS Server, Please Read

We wanted to inform you of a security incident we recently identified affecting your GoDaddy VPS server.

As part of our ongoing security detection and monitoring, our security team identified that your server hosted in VPS was infected with malware that allowed an unauthorized third party remote access to your server over Secure Shell (SSH). The malware replaced binaries (ssh, sshd) associated with Secure Shell (SSH) process running on your server with malicious binaries that allowed them access to the system without detection. This variant of malware also had the ability to capture SSH passwords if someone logged into the system over SSH. Our security team determined that the unauthorized third party added this malware to your server in October of 2019.

We have mitigated the issue by eliminating the malware from your server and have reinstalled packages containing known good SSH binaries. The scope of this incident is confined to your server in VPS and did not impact your main GoDaddy.com customer account or any other service you may have with GoDaddy.

We also conducted a thorough review and did not see any evidence or indication of activity from the unauthorized third party in the past 90 days.

As a precaution, you will need to reset all credentials for your server including your SSH passwords and keys upon your next log-in. If you use the same password for other accounts, we recommend you change your password to those accounts as well and follow data security best practices when doing so, including choosing a strong and unique password, changing that password regularly, and enabling multi-factor authentication where available.

Finally, we also recommend you conduct an audit of your server for any other unwanted or modified files that we did not detect.

We apologize for any inconvenience this may cause.

If you have any questions, or need further assistance, please contact support at <insert contact us page>.

The GoDaddy Security Team

[For Customers With Backups]

SUBJECT: Security Incident Impacting Your GoDaddy VPS Server, Please Read

We wanted to inform you of a security incident we recently identified affecting your GoDaddy VPS server.

As part of our ongoing security detection and monitoring, our security team identified that your server hosted in VPS was infected with malware that allowed an unauthorized third party remote access to your server over Secure Shell (SSH). The malware replaced binaries (ssh, sshd) associated with Secure Shell (SSH) process running on your server with malicious binaries that allowed them access to the system without detection. This variant of malware also had the ability to capture SSH passwords if someone logged into the system over SSH. Our security team determined that the unauthorized third party added this malware to your server in October of 2019.

We have mitigated the issue by eliminating the malware from your server and have reinstalled packages containing known good SSH binaries. The scope of this incident is confined to your server in VPS and did not impact your main GoDaddy.com customer account or any other service you may have with GoDaddy.

We also conducted a thorough review and did not see any evidence or indication of activity from the unauthorized third party in the past 90 days.

As a precaution, you will need to reset all credentials for your server including your SSH passwords and keys upon your next log-in. If you use the same password for other accounts, we recommend you change your password to those accounts as well and follow data security best practices when doing so, including choosing a strong and unique password, changing that password regularly, and enabling multi-factor authentication where available.

It is important to note that any malicious binaries that were on your server will also be present in any server backup. This includes, but is not limited to, "on demand" backups that you have requested through your server dashboard. We have removed any affected backups from your account. If you need to create a new backup, please log into your server dashboard. If the removed backup contained important information that you need access to, please contact our support team and we can assist with the recovery of these files for up to 90 days.

Finally, we also recommend you conduct an audit of your server for any other unwanted or modified files that we did not detect.

We apologize for any inconvenience this may cause.

If you have any questions, or need further assistance, please contact support at <insert contact us page>.

The GoDaddy Security Team