HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-PALOALTO*
System Identifier: Server name, services hosted, and IP Address:	*PALO ALTO*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	2/23/19 19:30

Note: Each system will use its own journal.
Use one row for each change.

Log Number	Line Number	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-PALOALTO	1	CCN-9-E-1000	Emergency	Removed unauthorized user from system	Deleted an unauthorized user from the device.	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	2	CCN-9-E-1001	Emergency	Created firewall rule to allow authorized services	Added a firewall rule to allow HTTPS and HTTP traffic to the Phantom server externally	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	3	CCN-9-E-1002	Emergency	Created firewall rule to allow authorized services	Added a firewall rule to allow Splunk, HTTPS, and HTTP traffic to the Phantom server externally	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	4	CCN-9-E-1003	Emergency	Created firewall rule to allow authorized services	Added a firewall rule to allow DNS traffic to the DNS server externally	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	5	CCN-9-E-1004	Emergency	Created firewall rule to allow authorized services	Added a firewall rule to allow HTTP traffic to the Ecom server externally	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	6	CCN-9-E-1005	Emergency	Created firewall rule to allow authorized services	Added a firewall rule to allow DNS traffic to the Active Directory server externally	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	7	CCN-9-E-1006	Emergency	Created firewall rule to allow authorized services	Added a firewall rule to allow pop3, smtp, and web traffic to the Linux Webmail server externally	Only authorized users should have access to critical HAL infrastructure. With this change unauthorized users will be unable to authenticate with the Palo Alto Firewall.
9-PALOALTO	8	CCN-9-E-1007	Emergency	Created firewall rule to block unnecessary traffic	Added a firewall rule to block SSH traffic to all servers externally	All management of HAL servers is done using console access, therefore SSH access is unnecessary.
9-PALOALTO	9	CCN-9-E-1008	Emergency	Created firewall rule to block unnecessary traffic	Added a firewall rule to block all unnecessary inbound network traffic	Since all necessary external services have been explicitly whitelisted, this rule acts to enable the whitelist and block all other traffic.
9-PALOALTO	10	CCN-9-E-1009	Emergency	Created firewall rule to block a malicious IP address	Added a firewall rule to block 10.0.1.69 from accessing internal systems	This IP Address was seen as malicious by system administrators and was thus blocked from accessing HAL systems
9-PALOALTO	11	CCN-29-E-1010	Emergency	Created firewall rule to block a malicious IP address	Added a firewall rule to block 10.0.0.102 from accessing internal systems	This IP Address was seen as malicious by system administrators and was thus blocked from accessing HAL systems
9-PALOALTO	12	CCN-29-E-1011	Emergency	Created firewall rule to block a malicious IP address	Added a firewall rule to block 10.0.0.100 from accessing internal systems	This IP Address was seen as malicious by system administrators and was thus blocked from accessing HAL systems

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-Windows8.1*
System Identifier: Server name, services hosted, and IP Address:	*Windows 8.1, 172.20.242.100*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	2/23/19 19:30

Note: Each system will use its own journal.
Use one row for each change.

Log Number	Line Number	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-Windows8.1	1	CCN-9-E-1301	Emergency	Changed Passwords	02/23/2019 03:10 Many user account passwords have been changed in case the password was compromised.	In the case that an adversary had the user password, this password reset removes their ability to reauthenticate.
9-Windows8.1	2	CCN-9-E-1302	Emergency	Disabled User Accounts	2/23/2019 3:30 Non-necessary user accounts "Administrator" and "goofclod" were disabled to reduce attack surface on the machine.	This will prevent adversaries from accessing insecure user accounts and using them as attack vectors.
9-Windows8.1	3	CCN-9-E-1303	Emergency	Enabled System Firewall	02/23/2019 03:35 Windows Firewall was enabled as a precautionary step to deal with rouge network traffic that is unexpected for this system. In the case that a service becomes unavailable, rules will be added to the firewall to re-allow normal operation. Firewall may be disabled entirely if necessary.	No negative impact is expected. This change can drastically reduce the attack surface on this system and ultimately the network.
9-Windows8.1	4	CCN-9-E-1304	Emergency	Created User Accounts	2/23/2019 3:45 Two administrative user accounts, "beckup" and "user", were created to allow team members to administrate the machine in the case that default administrator account is compromised. These accounts can easily be removed or locked if this change needs to be reverted.	Through this change will marginally increase the attack surface of the server, it will not do so in any meaningful way, because a secure and confidential password will protect the new account. The existence of this account will assist in recovery procedures should the server be compromised.
9-Windows8.1	5	CCN-9-E-1305	Emergency	Password Rotation	2/23/2019 7:00 All enabled local users ("User" and "beckup") had their passwords rotated. This was done in the case that an account had been compromised, removing the chance that an adversary had obtained valid credentials.	In the case that an adversary had the user password, this password reset removes their ability to reauthenticate.
9-Windows8.1	6	CCN-9-E-1306	Emergency	Installed the Wireshark	The Wireshark application was installed in	Any malicious activity that is

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-ADWin2008R2*
System Identifier: Server name, services hosted, and IP Address:	*AD, AD/DNS, 172.20.242.200*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	2/23/19 19:30

Note: Each system will use its own journal.
Use one row for each change.

Log Number	Line Number	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-ADWin2008R2	1	CCN-9-E-1151	Emergency	Changed Passwords	02/23/2019 3:00 PM Administrator account password has been changed in case the password has been compromised.	In the case that an adversary had the Administrator password, this password reset removes their ability to reauthenticate.
9-ADWin2008R2	2	CCN-9-E-1152	Emergency	Disabled User Account	02/23/2019 03:01 The user account proftp has been disabled, because it is unnnecessary or malicous. Every use account on a system increases the attack surface, so removing	This will have no negative impact to the bussiness unit, and reduces the attack surface of this system.
9-ADWin2008R2	3	CCN-9-E-1153	Emergency	Added Backup Administ	02/23/2019 3:02 PM An additional administrator account was added, msthubin that will allow access to this server by designed members of our HAL auditing team in case the default administrator account is compromised. This account can easily be removed or locked if this change needs to be reverted.	Though this change will marginally increase the attack surface of the server, it will not do so in any meaningful way, because a secure and confidential password will protect the new account. The existance of this account will assist in recovery procedures should the server be compromised.
9-ADWin2008R2	4	CCN-9-E-1154	Emergency	Disabled User Account	02/23/2019 03:05 The user account proftp has been disabled, because it is unnnecessary or malicous. Every use account on a system increases the attack surface, so removing	This will have no negative impact to the bussiness unit, and reduces the attack surface of this system.
9-ADWin2008R2	5	CCN-9-E-1155	Emergency	Uninstalled WinSCP Potentially unwanted software	02/23/2019 03:15 Uninstalled WinSCP progam due to its potential for masking malicous activity and its unnecessary use of system resoruces. This program can be re-installed if necessary.	Uninstalling the WinSCP program incrased the efficiency of the business unit by reducing the amount required infrastrure resources and reduced the attack surface on programs not needed to accomplish the business mission.
9-ADWin2008R2	6	CCN-9-E-1156	Emergency	Added Team Member User Accounts	02/23/2019 3:20 Added team member user accounts to the system to allow all of the members of the b usiness unit to access the services on this servers. These users can be easily removed in the same manner they were added if necessary.	No negative impact is expected. All of the users were given a secure password that corresponds to HAL policy, and were only given permission to access the appropiate resources.
9-ADWin2008R2	7	CCN-9-E-1157	Emergency	Installed MalwareBytes Antivirus	02/23/2019 3:25 Antivirus was installed to detect and mitigate agaisnt common malicous files and applications. The antivirus program users a combination of signature and behavior detection methods, which could cause a false positive. The default action is to quarantine the detected item instead of automatic removal, so that files and applications can be quickly whitelisted for future scans	By deploying an antivirus application, we increase the detection of commonly used malicous tools which may be used to compromise the security of the system. This change should be mostly transparent to our end users.
9-ADWin2008R2	8	CCN-9-E-1158	Emergency	Uninstalled IIS	02/23/2019 4:00 Microsoft Internet Information Services has been uninstalled from this system. This feature can be re-added if necessary.	Uninstalling IIS from this server reduces the attack surface of this system by disabling unnecessary web connectivity.
9-ADWin2008R2	9	CCN-9-E-1159	Emergency	Changed Passwords	02/23/2019 4:03 PM Administrator account password has been changed in case the password has been compromised.	In the case that an adversary had the Administrator password, this password reset removes their ability to reauthenticate.
9-ADWin2008R2	10	CCN-9-E-1160	Emergency	Enabled Applocker	02/23/2019 4:45 PM AppLocker was enabled to prevent malicous applications from running. Windows AppLocker uses a combination of signature and path comparisions to see if a particular application is allowed to run; if not on t he whitelistt the application cannot run. The default action is to prevent the execution of the unrecognized application; however if the application is desired it can be quickly whitelisted for use. AppLocker can be disabled if this change needs to be reverted or gets in the way of bussienss requirements.	Unrecognized applications and executables will be prohibited from running, but known customer facing services are still alllowed. Thereforce, no business impact is expected.
9-ADWin2008R2	11	CCN-9-E-1161	Emergency	Changed Passwords	02/23/2019 5:00 PM Administrator account password has been changed in case the password has been compromised.	In the case that an adversary had the Administrator password, this password reset removes their ability to reauthenticate.
9-ADWin2008R2	12	CCN-9-E-1162	Emergency	Edited the zone transfe	Disabled Zone transfers from the DNS servers	We do not currently expect a business impa
9-ADWin2008R2	13	CCN-9-E-1163	Emergency	Malware was removed f	The Malwarebytes application noticed Malwa	System is more secure with the Malware.

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-Windows10*
System Identifier: Server name, services hosted, and IP Address:	*Windows 10, 172.31.9.5*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	2/23/19 19:30

Note: Each system will use its own journal.
Use one row for each change.

Log Number	Line Number	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-Windows10	1	CCN-9-E-1305	Emergency	Changed Passwords	02/23/2019 03:10 Many user account passwords have been changed in case the password was compromised.	In the case that an adversary had the user password, this password reset removes their ability to reauthenticate.
9-Windows10	2	CCN-9-E-1306	Emergency	Disabled User Account	2/23/2019 3:30 Non-necessary user account "Administrator" was disabled to reduce attack surface on the machine.	This will prevent adversaries from accessing insecure user accounts and using them as attack vectors.
9-Windows10	3	CCN-9-E-1307	Emergency	Enabled System Firewall	02/23/2019 03:35 Windows Firewall was enabled as a precautionary step to deal with rouge network traffic that is unexpected for this system. In the case that a service becomes unavailable, rules will be added to the firewall to re-allow normal operation. Firewall may be disabled entirely if necessary.	No negative impact is expected. This change can drastically reduce the attack surface on this system and ultimately the network.
9-Windows10	4	CCN-9-E-1308	Emergency	Created User Account	2/23/2019 3:45 An administrative user account, "backup", was created to allow team members to administrate the machine in the case that default administrator account is compromised. This account can easily be removed or locked if this change needs to be reverted.	Through this change will marginally increase the attack surface of the server, it will not do so in any meaningful way, because a secure and confidential password will protect the new account. The existence of this account will assist in recovery procedures should the server be compromised.
9-Windows10	5	CCN-9-E-1309	Emergency	Password Rotation	2/23/2019 6:55 All enabled local users ("minion" and "backup") had their passwords rotated. This was done in the case that an account had been compromised, removing the chance that an adversary had obtained valid credentials.	In the case that an adversary had the user password, this password reset removes their ability to reauthenticate.

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-Splunk*
System Identifier: Server name, services hosted, and IP Address:	*Splunk, 172.20.241.20*
Date and time log was started:	02/23/19 03:00 PM
Date and time log was completed:	2/23/19 19:30

Note: Each system will use its own journal.
Use one row for each change.

Log Number	ine Numbe	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-Splunk	1	CCN-9-E-1000	Emergency	Disabled Sshd	I disabled the program openssh server which is in charge of allowing remote users to connect and manage the server.	Remote users will no longer be able to login and manage the server
9-Splunk	2	CCN-9-E-1001	Emergency	Disabled Crond	I disabled the program crond which is in charge of running scheduled tasks.	Scheduled tasks malicious and no will not run
9-Splunk	3	CCN-9-E-1002	Emergency	Added Firewall Rules	02/23/2019 15:05:21 A firewall was added to prevent access to services that are not required and could be potentially be used to aid in a breach.	Unexpected traffic will not be allowed into the server.
9-Splunk	4	CCN-9-E-1003	Emergency	Changed passwords	02/23/2019 15:03:41 User account password has been modified in case the previous password was comprised.	The previous account passwords will not work.
9-Splunk	5	CCN-9-E-1004	Emergency	Deleted old ssh keys	02/23/2019 15:10:28 Some of the old users had there ssh keys still on the system which would allow them to login without a password. These keys have been removed.	Old users will not be able to login with there ssh keys.
9-Splunk	6	CCN-9-E-1005	Emergency	Changed passwords	02/23/2019 17:03 The root account password has been changed. HAL Company policy is to rotate passwords regularly.	If an attacker compromised this host, their credentials would no longer work for the root user.
9-Splunk	6	CCN-9-E-1006	Emergency	Audited Running Proces	The running processes on the host has been audited. Services running that are not necessary have been stopped.	This reduces the attack surface of the host.
9-Splunk	6	CCN-9-E-1007	Emergency	Scanned the system for	The filesystem has been audited for	This removes any Malware a

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-Fedora*
System Identifier: Server name, services hosted, and IP Address:	*Fedora-Mail-172.20.241.40*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	2/23/19 19:30

Note: Each system will use its own journal.
Use one row for each change.

Log Number	ine Numbe	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-Fedora	1	CCN-9-E-1005	Emergency	Disabled Sshd	02/23/2019 15:00:23 I disabled the program openssh server which is in charge of allowing remote users to connect and manage the server.	Remote users will no longer be able to login and manage the server
9-Fedora	2	CCN-9-E-1006	Emergency	Disabled Crond	02/23/2019 15:00:23 I disabled the program crond which is in charge of running scheduled tasks.	Scheduled tasks malicious and no will not run
9-Fedora	3	CCN-9-E-1007	Emergency	Added Firewall Rules	02/23/2019 15:05:21 A firewall was added to prevent access to services that are not required and could be potentially be used to aid in a breach.	Unexpected traffic will not be allowed into the server.
9-Fedora	4	CCN-9-E-1008	Emergency	Changed passwords	02/23/2019 15:03:41 User account password has been modified in case the previous password was comprised.	The previous account passwords will not work.
9-Fedora	5	CCN-9-E-1009	Emergency	Deleted old ssh keys	02/23/2019 15:10:28 Some of the old users had there ssh keys still on the system which would allow them to login without a password. These keys have been removed.	Old users will not be able to login with there ssh keys.
9-Fedora	6	CCN-9-E-1010	Emergency	Changed passwords	02/23/2019 17:03: The root account password has been changed. HAL Company policy is to rotate passwords regularly.	If an attacker compromised this host, their credentials would no longer work for the root user.
9-Fedora	6	CCN-9-E-1011	Emergency	Audited Running Proces	The running processes on the host has been audited. Services running that are not necessary have been stopped.	This reduces the attack surface of the host.
9-Fedora	6	CCN-9-E-1012	Emergency	Scanned the system for	The filesystem has been audited for	This removes any Malware a

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-Phantom*
System Identifier: Server name, services hosted, and IP Address:	*Phantom, 172.20.240.10*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	02/23/19 07:30 PM

Note: Each system will use its own journal.
Use one row for each change.

Log Number	ine Numbe	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-Phantom	1	CCN-9-E-1010	Emergency	Disabled Sshd	02/23/2019 15:00:23 I disabled the program openssh server which is in charge of allowing remote users to connect and manage the server.	Remote users will no longer be able to login and manage the server
9-Phantom	2	CCN-9-E-1011	Emergency	Disabled Crond	02/23/2019 15:00:23 I disabled the program crond which is in charge of running scheduled tasks.	Scheduled tasks malicious and no will not run
9-Phantom	3	CCN-9-E-1012	Emergency	Added Firewall Rules	02/23/2019 15:05:21 A firewall was added to prevent access to services that are not required and could be potentially be used to aid in a breach.	Unexpected traffic will not be allowed into the server.
9-Phantom	4	CCN-9-E-1013	Emergency	Changed passwords	02/23/2019 15:03:41 User account password has been modified in the previous password was comprised.	The previous account passwords will not work.
9-Phantom	5	CCN-9-E-1014	Emergency	Deleted old ssh keys	02/23/2019 15:10:28 Some of the old users had there ssh keys still on the system which would allow them to login without a password. These keys have been removed.	Old users will not be able to login with there ssh keys.
9-Phantom	6	CCN-9-E-1015	Emergency	Changed passwords	02/23/2019 17:03: The root account password has been changed. HAL Company policy is to rotate passwords regularly.	If an attacker compromised this host, their credentials would no longer work for the root user.
9-Phantom	6	CCN-9-E-1016	Emergency	Audited Running Proces	The running processes on the host has been audited. Services running that are not necessary have been stopped.	This reduces the attack surface of the host.
9-Phantom	6	CCN-9-E-1017	Emergency	Scanned the system for	The filesystem has been audited for	This removes any Malware a

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-CENTOS*
System Identifier: Server name, services hosted, and IP Address:	*Centos, Ecom, 172.20.241.30*
Date and time log was started:	2/23/19 15:00
Date and time log was completed:	02/23/19 07:30 PM

Note: Each system will use its own journal.
Use one row for each change.

Log Number	ine Numbe	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-CENTOS	1	CCN-29-E-1015	Emergency	Rotated passwords for the web application	The default administrative credentials for the ecommerce application were changed in order to ensure the ongoing security of the hosted service.	Because the passwords to the application were changed from their defaults, an attacker would be unable to access the administration panel using the easily guessable (and often well documented) default password.
9-CENTOS	2	CCN-29-E-1016	Emergency	Rotated passwords for local users	Credentials for the system's local administrative users (which are distinct from the web application) were updated to ensure the ongoing security of the underlying operating system.	Because the passwords to the host operating system were changed from their defaults, an attacker would be unable to accessp privileged accounts using the easily guessable (and often well documented) default password.
9-CENTOS	3	CCN-29-E-1017	Emergency	Applied a hardened PHP configuration	The PHP service, which hosts the web application's frontend, was initially configured using insecure default directives. These were updated to include a host of more robust and granular permissions in order to limit lateral movement into the host operating system on the part of an attacker via the web application.	Because the PHP configuration was hardened, the ability of an attacker to perform attacks on the underlying operating system was severely limited. Because these changes only affect malicious PHP code, it will not inhibit the normal function of the ecommerce frontend in any way.
9-CENTOS	4	CCN-9—E-1018	Emergency	Removed preexisting authorized_keys	Preexisting authorized_keys files were discovered on the host system. Because these were unknown to the administrator at the time they were observed, these keys were removed.	Removing old authorized_keys files helps to ensure the continued security and integrity of the host system. As a result of these changes, stronger access controls are now enforced on the host
9-CENTOS	5	CCN-29-E-1019	Emergency	Disabled the SSH service	The unnecessary OpenSSH Server service was disabled.	Disabling and removing unnecessary services is considered to be best practice, and OpenSSH is no exception. As a result of this change, the overall attack surface of the host system has been minimized.
9-CENTOS	6	CCN-9-E-1020	Emergency	Scanned the system for	The filesystem has been audited for	This removes any Malware a system may

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-DEBIAN*
System Identifier: Server name, services hosted, and IP Address:	*Debian, Mysql, 172.20.240.20*
Date and time log was started:	02/23/19 03:00 PM
Date and time log was completed:	02/23/19 04:30 PM

Note: Each system will use its own journal.
Use one row for each change.

Log Number	ine Numbe	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-DEBIAN	1	CCN-9-E-1020	Emergency	Disabled Sshd	I disabled the program openssh server which is in charge of allowing remote users to connect and manage the server.	Remote users will no longer be able to login and manage the server
9-DEBIAN	2	CCN-9-E-1021	Emergency	Disabled Crond	I disabled the program crond which is in charge of running scheduled tasks.	Scheduled tasks malicious and no will not run
9-DEBIAN	3	CCN-9-E-1022	Emergency	Added Firewall Rules	02/23/2019 15:05:21 A firewall was added to prevent access to services that are not required and could be potentially be used to aid in a breach.	Unexpected traffic will not be allowed into the server.
9-DEBIAN	4	CCN-9-E-1023	Emergency	Changed passwords	02/23/2019 15:03:41 User account password has been modified in the previous password was comprised.	The previous account passwords will not work.
9-DEBIAN	5	CCN-9-E-1024	Emergency	Deleted old ssh keys	02/23/2019 15:10:28 Some of the old users had there ssh keys still on the system which would allow them to login without a password. These keys have been removed.	Old users will not be able to login with there ssh keys.
9-DEBIAN	6	CCN-9-E-1025	Emergency	Changed passwords	02/23/2019 17:03: The root account password has been changed. HAL Company policy is to rotate passwords regularly.	If an attacker compromised this host, their credentials would no longer work for the root user.
9-DEBIAN	6	CCN-9-E-1026	Emergency	Audited Running Proces	The running processes on the host has been audited. Services running that are not necessary have been stopped.	This reduces the attack surface of the host.
9-DEBIAN	6	CCN-9-E-1027	Emergency	Scanned the system for	The filesystem has been audited for	This removes any Malware a

HAL - Change Control Journal

Journal Identifier: Region letter & unique journal code:	*9-Ubuntu*
System Identifier: Server name, services hosted, and IP Address:	*Ubuntu,DNS, 172.20.242.10*
Date and time log was started:	02/23/19 03:00 PM
Date and time log was completed:	02/23/19 04:30 PM

Note: Each system will use its own journal.
Use one row for each change.

Log Number	ine Numbe	Change Request Number	Change Type	Change Summary	Change Details	Impact / Outcome
This is a unique ID for this log within the HAL region, to enable merging and sorting.	*Unique line number for each change item, to enable merging and sorting.*	*For example CCN-12-E-1001*	*Routine or Emergency*	*Provide a brief summary of the change not to exceed 75 words.*	*Provide a complete explanation of the change. If this as for a routine change this duplicates the information on the change request form in every particular. It must include the roll back planning that was done. If emergency change, justify use of emergency change process. BE CERTAIN to include specific dates and times of all notable events in the progression of this change item.*	*Fully explain the outcome of the change and the impact of the change on the business unit.*
9-Ubuntu	1	CCN-9-E-1025	Emergency	Disabled Sshd	I disabled the program openssh server which is in charge of allowing remote users to connect and manage the server.	Remote users will no longer be able to login and manage the server
9-Ubuntu	2	CCN-9-E-1026	Emergency	Disabled Crond	I disabled the program crond which is in charge of running scheduled tasks.	Scheduled tasks malicious and no will not run
9-Ubuntu	3	CCN-9-E-1027	Emergency	Added Firewall Rules	02/23/2019 15:05:21 A firewall was added to prevent access to services that are not required and could be potentially be used to aid in a breach.	Unexpected traffic will not be allowed into the server.
9-Ubuntu	4	CCN-9-E-1028	Emergency	Changed passwords	02/23/2019 15:03:41 User account password has been modified in the previous password was comprised.	The previous account passwords will not work.
9-Ubuntu	5	CCN-9-E-1029	Emergency	Deleted old ssh keys	02/23/2019 15:10:28 Some of the old users had there ssh keys still on the system which would allow them to login without a password. These keys have been removed.	Old users will not be able to login with there ssh keys.
9-Ubuntu	6	CCN-9-E-1030	Emergency	Changed passwords	02/23/2019 17:03: The root account password has been changed. HAL Company policy is to rotate passwords regularly.	If an attacker compromised this host, their credentials would no longer work for the root user.
9-Ubuntu	6	CCN-9-E-1031	Emergency	Audited Running Proces	The running processes on the host has been audited. Services running that are not necessary have been stopped.	This reduces the attack surface of the host.
9-Ubuntu	6	CCN-9-E-1032	Emergency	Scanned the system for	The filesystem has been audited for	This removes any Malware a